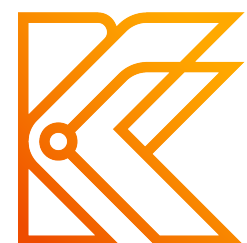


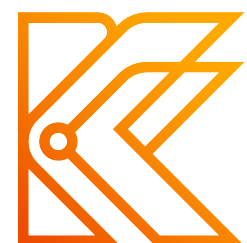
# Dicas **Óbvias** (ou não) para quem trabalha com Redes de computadores

Nível  
Básico

\*Não é necessário nenhum conhecimento prévio para acompanhar essa apresentação.



# Palestra pós almoço numa sexta-feira





# Quem sou eu?



Antes de tudo obrigado;

Meu nome é Gustavo Kalau;

Galera que tá na live, compartilha o link ai nos grupos de ZAP/Telegram, se inscreva do canal do NIC, comenta e deixa o like.



Sou formado em Sistemas de Informação pela PUC/MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC/MG, atuo há mais de 14 anos com redes de computadores;

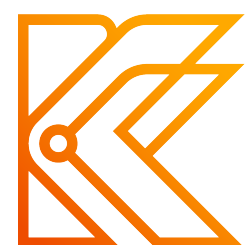
Trabalhei com operação de rede WAN/LAN Enterprise durante 11 anos na Empresa de Informática e Informação do Município de Belo Horizonte – Prodabel, saindo de uma rede puramente L2 para uma rede MPLS com infraestrutura própria (+-1000km fibra) e dois DCs;

Fui professor universitário por 8 anos em instituições privadas como PUC/MG e Estácio em cursos de graduação e pós-graduação;

Desde de 2016 ministra treinamentos em minha própria empresa de ensino a distância;

Tenho algumas certificações na área como: CCIE R&S #60243, CCNA , CCNP Ent, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials;

Moro em BH, pratico corrida de rua e torço pro Galo.





# Minha Empresa - Gustavo Kalau Treinamento

Canal no YouTube criado em 2015;

Cerca de 70K de inscritos, 437 vídeos, mais de 3 milhões de visualizações com cursos gratuitos, workshops, entrevistas e dicas da área de redes;

17K seguidores no Instagram, posts descontraídos e caixinhas de perguntas quase todos os dias (11K seguidores no LinkedIn);

No meio de 2016 abri uma empresa e comecei a vender meus cursos em plataforma própria;

Em 2019 decidi montar um estúdio em uma sala comercial;

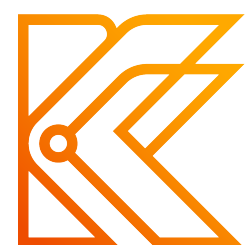
No final de 2021 “larguei tudo” para me dedicar na empresa;

3452 alunos ativos em diversos países, 8 cursos gravados (CCNA, CCNP, Fortigate, Descomplicando o BGP, OSPF, MPLS), 1340 cursos vendidos em 2024, reembolso 23 (2%), aumento de 15% com relação a 2023, zero reclamações no Reclame Aqui. Empresas e Instrutores compram meus treinamentos. Tem Lojinha de camisetas.

One person business model.

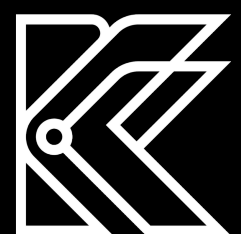


Orquídea de Lego



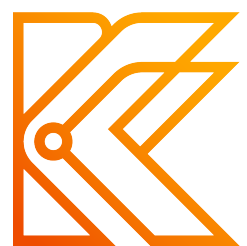


“Esta é uma obra de ficção,  
qualquer semelhança com nomes,  
pessoas, fatos ou situações da vida  
real terá sido mera coincidência”



Dica **óbvia** #1:

**Faça a topologia da sua rede e mantenha sempre atualizada.**





New Message



To cliente@redegrandecomplexa.com

Subject Enviar topologia referente ao Ticket Urgente #451397

Olá Fulano,

Referente ao ticket Urgente #451397 aberto por você, **precisamos da topologia da rede** conforme informado no próprio ticket e conforme conversado na call realizada para tratarmos do problema, reforçamos que devido a complexidade do ambiente é improvável que o problema seja resolvido sem que tenhamos uma visibilidade detalhada do seu ambiente.

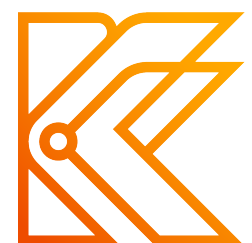
Obrigado e no aguardo.



@gustavokalau



SEND



RESPOSTA



Boa tarde,

Segue topologia em anexo conforme solicitado.

Aguardo atualização do ticket o quanto antes, a rede está com sérios problemas e isso afeta diretamente a nossa produção.

Obrigado.

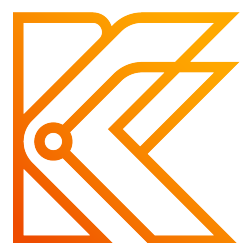


TopologiaCompleta Atualizada.jpg

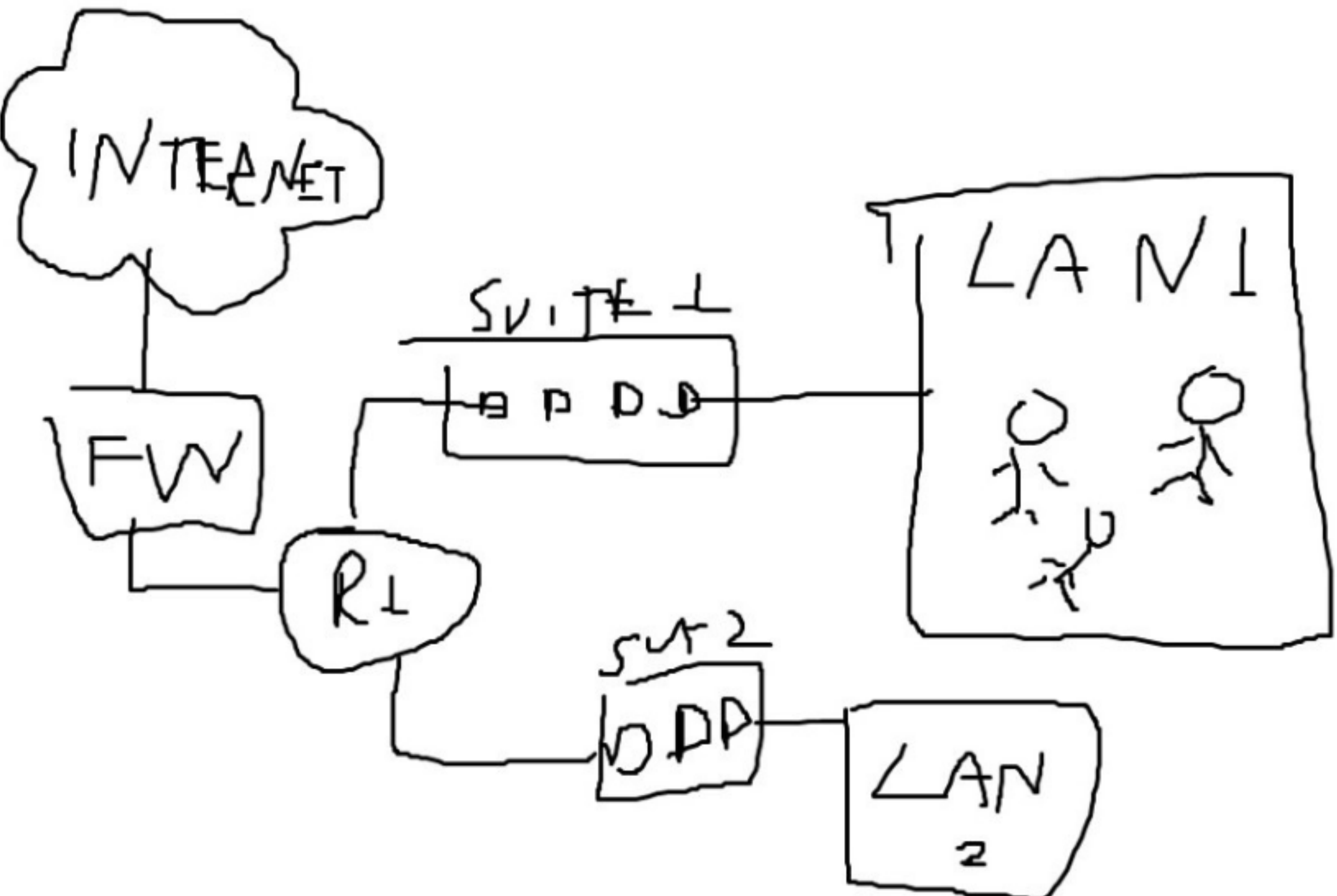
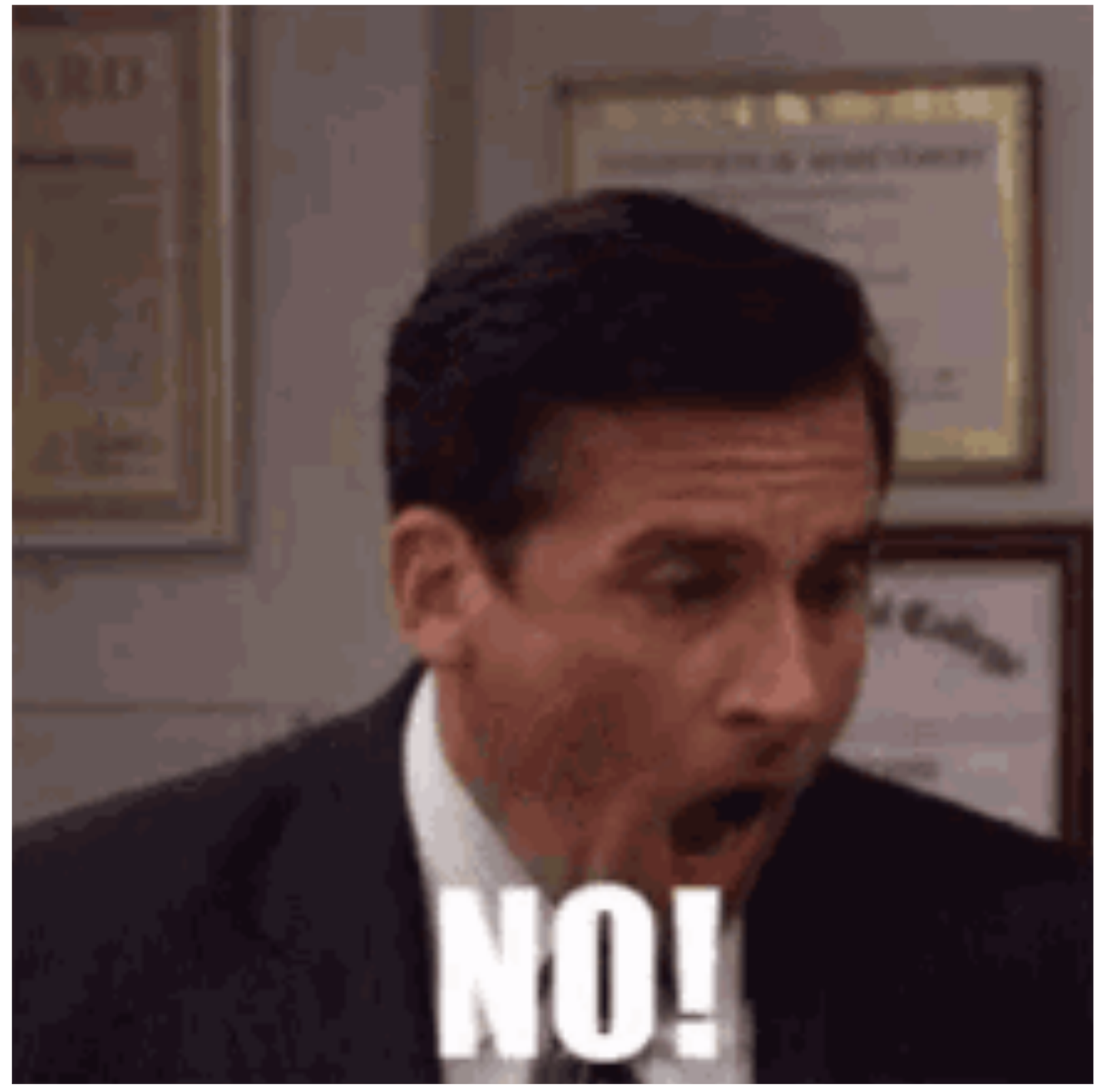
@gustavokalau



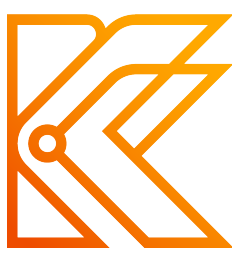
responder







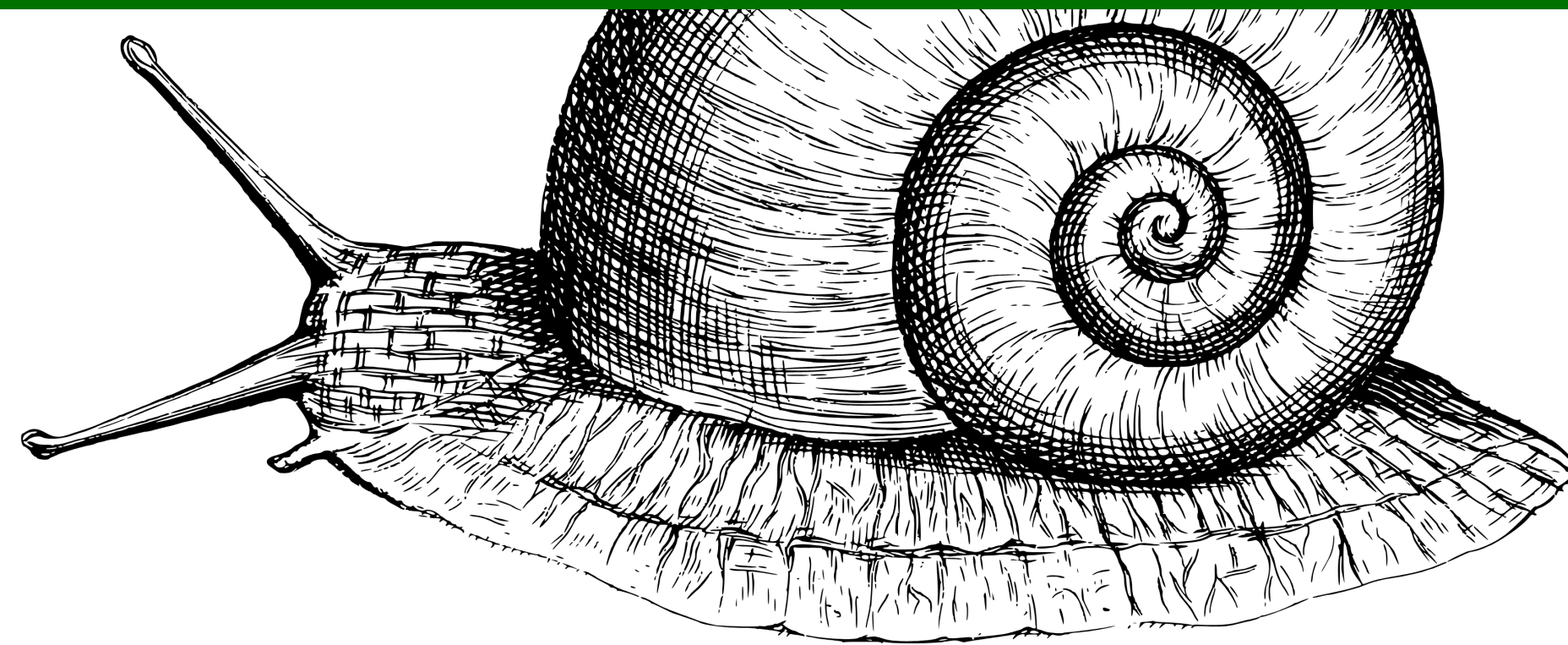
@gustavokalau



“A escassez é a mãe da criatividade”

@gustavokalau

FAKE - É UMA PIADA

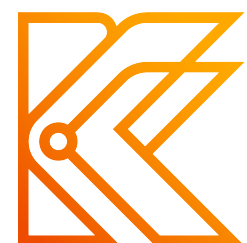


# Resolvendo Problemas

Em redes sem documentação

O'RIVEL

Angus MacGyver



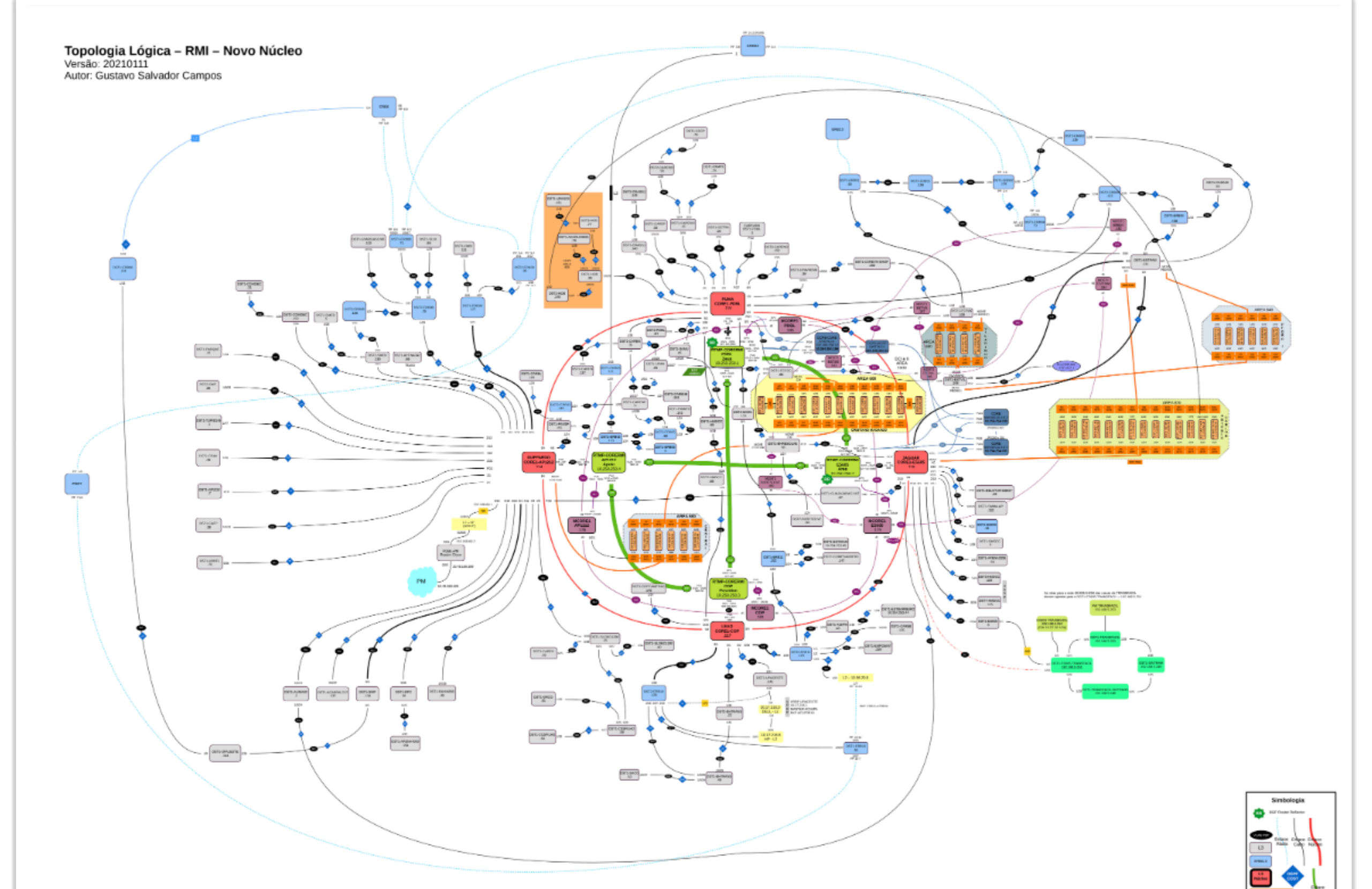
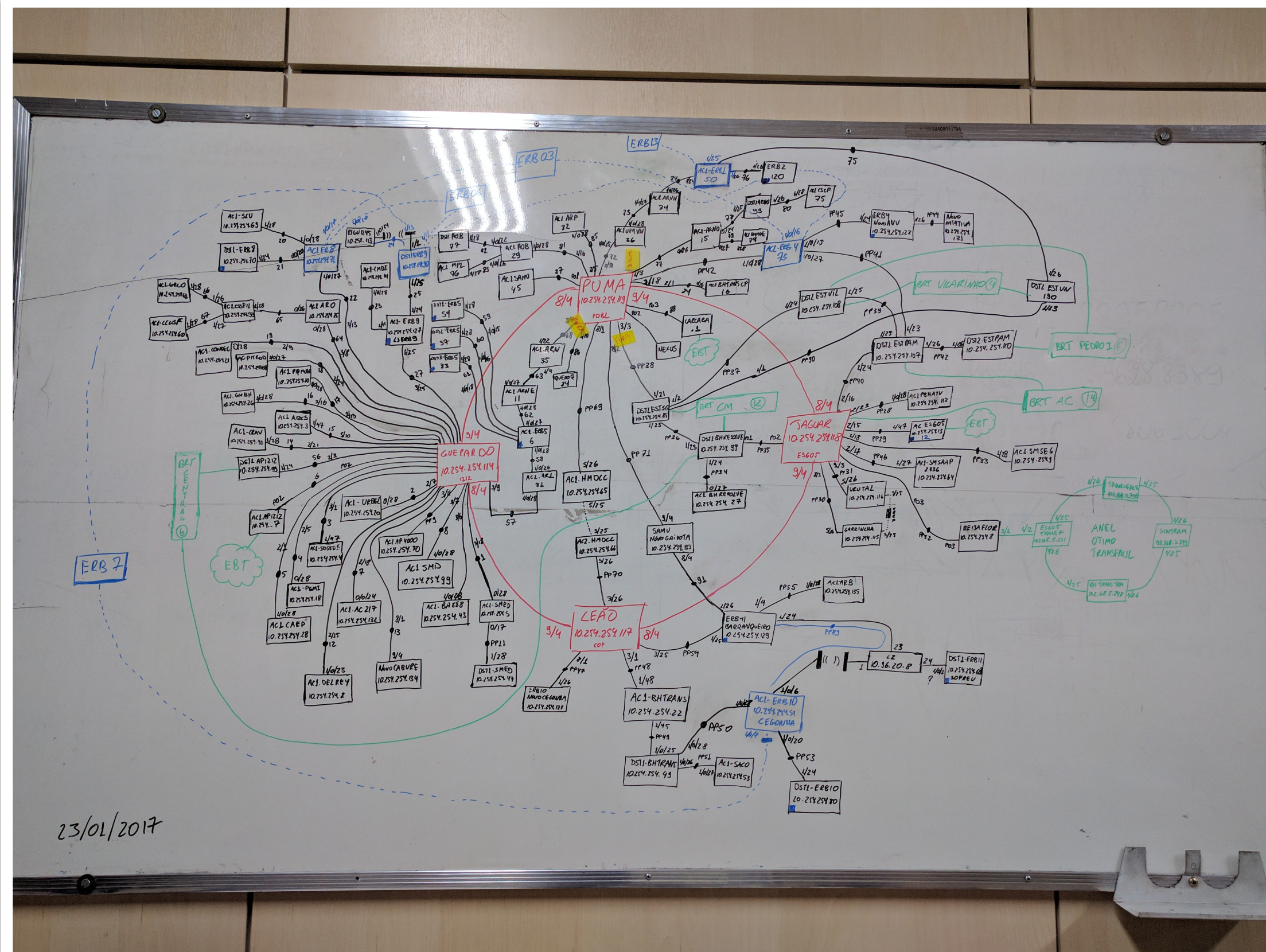


# Desenhe a sua rede, é sério

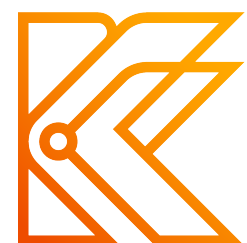


É o documento mais importante da sua rede (na minha opinião).

Trabalhar sem topologia é como dirigir a 200Km/h de noite e sem farol.

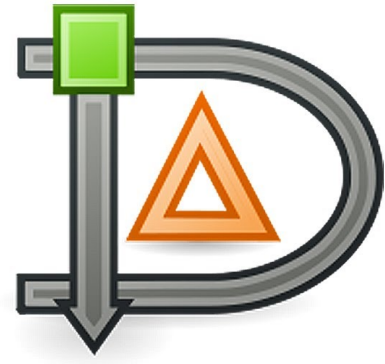


Entenda o fluxo básico do tráfego da sua rede, como o pacote X chega no lugar Y, por que ele usa essa rota? Como foi tomada essa decisão? Quais os protocolos envolvidos? Isso tá certo? Converse com as pessoas, tire dúvidas, seja interessado.

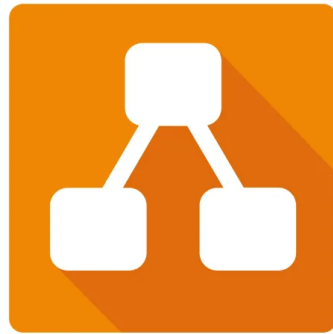




# Ferramenta é o que não falta



Dia



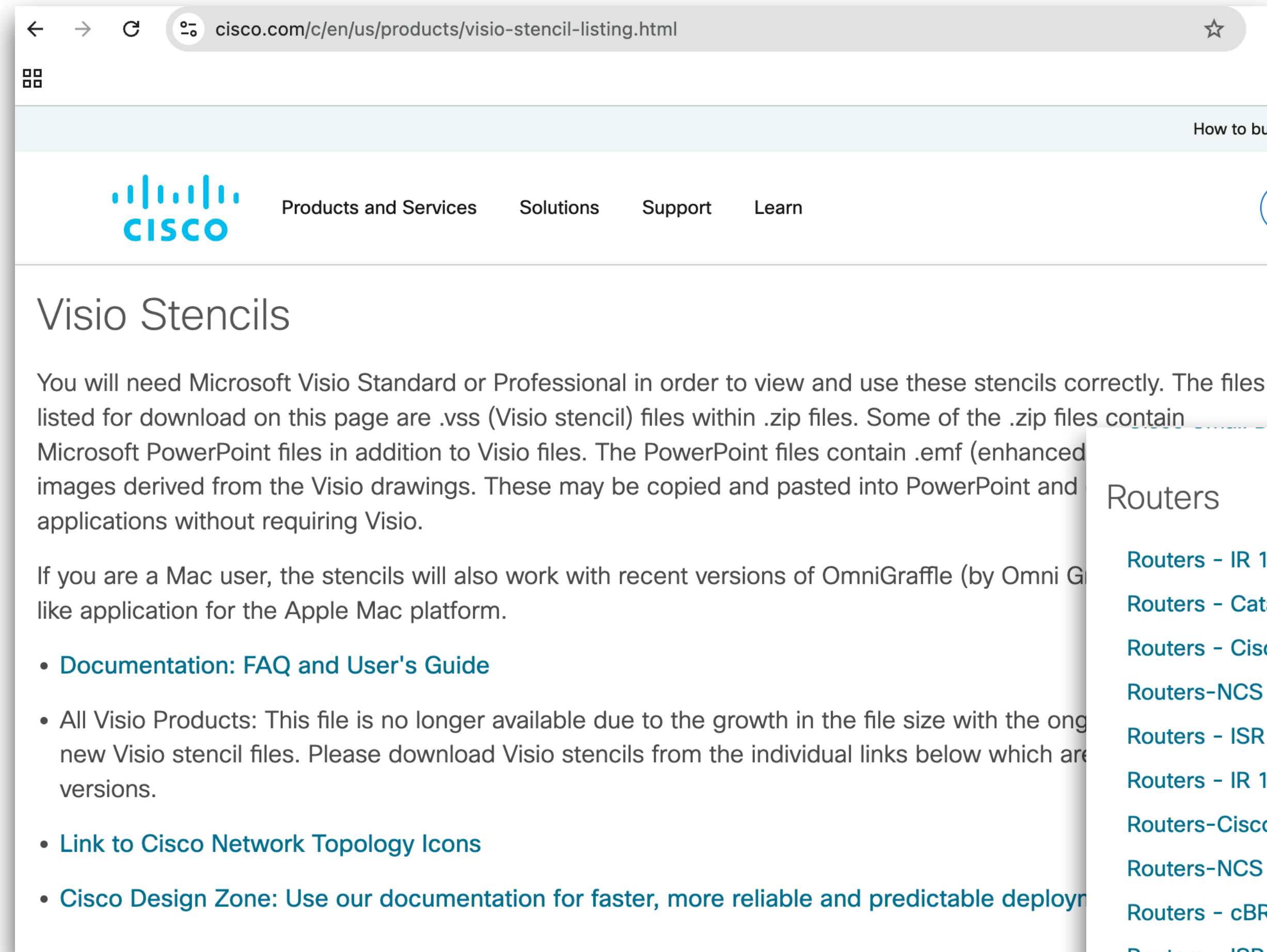
draw.io



Visio



PowerPoint



The screenshot shows a web browser window with the URL [cisco.com/c/en/us/products/visio-stencil-listing.html](https://cisco.com/c/en/us/products/visio-stencil-listing.html). The page title is "Visio Stencils". The main content area contains the following text:

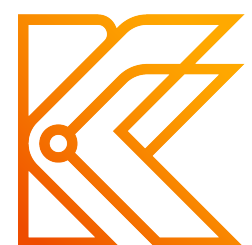
You will need Microsoft Visio Standard or Professional in order to view and use these stencils correctly. The files listed for download on this page are .vss (Visio stencil) files within .zip files. Some of the .zip files contain Microsoft PowerPoint files in addition to Visio files. The PowerPoint files contain .emf (enhanced images derived from the Visio drawings. These may be copied and pasted into PowerPoint and applications without requiring Visio.

If you are a Mac user, the stencils will also work with recent versions of OmniGraffle (by Omni Group) like application for the Apple Mac platform.

- [Documentation: FAQ and User's Guide](#)
- All Visio Products: This file is no longer available due to the growth in the file size with the ongoing new Visio stencil files. Please download Visio stencils from the individual links below which are the latest versions.
- [Link to Cisco Network Topology Icons](#)
- [Cisco Design Zone: Use our documentation for faster, more reliable and predictable deployment](#)

## Routers

- [Routers - IR 1800 \(ZIP - 2 MB\) 07/Dec/2023](#)
- [Routers - Catalyst 8000 \(ZIP - 3 MB\) 06/Oct/2021](#)
- [Routers - Cisco 8000 \(ZIP - 17 MB\) 07/Aug/2023](#)
- [Routers-NCS 560 \(ZIP - 3 MB\) 30/Jun/2021](#)
- [Routers - ISR 900 \(ZIP - 91 KB\) 24/Jul/2019](#)
- [Routers - IR 1101 \(ZIP - 111 KB\) 19/May/2019](#)
- [Routers-Cisco vEdge 5000 \(ZIP - 687 KB\) 29/Apr/2019](#)
- [Routers-NCS 540 \(ZIP - 7 MB\) 22/Nov/2021](#)
- [Routers - cBR-8 \(ZIP - 5 MB\) 29/Jul/2018](#)
- [Routers - ISR 1100 \(ZIP - 3 MB\) 29/Aug/2021](#)
- [Enterprise Network Compute System \(ENCS\) 5100 Series \(ZIP - 11 MB\) 06/Oct/2022](#)
- [Enterprise Network Compute System \(ENCS\) 5400 Series \(ZIP - 11 MB\) 06/Oct/2022](#)
- [Routers-NCS 5500 \(ZIP - 22 MB\) 06/Oct/2022](#)
- [Routers-NCS 6000 \(ZIP - 4 MB\) 18/Aug/2016](#)



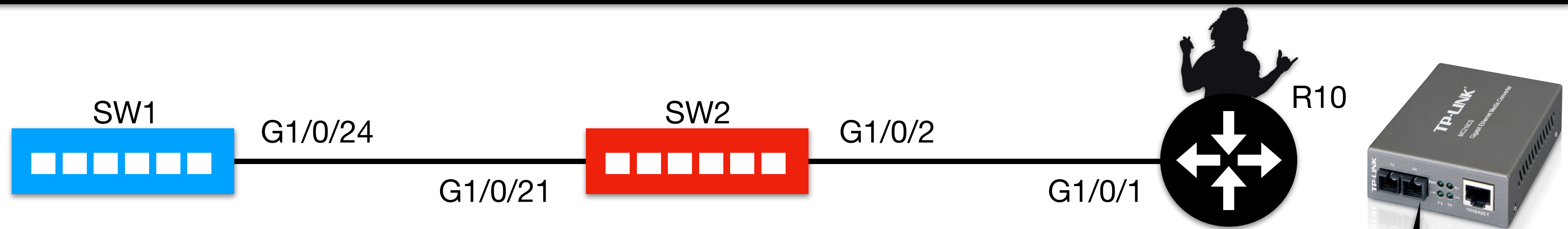


# CDP e LLDP para te ajudar

O CDP (Cisco Discovery Protocol) descobre informações básicas sobre roteadores e switches vizinhos sem precisar saber as senhas dos dispositivos vizinhos. (É um protocolo de cada 2). Utiliza o multicast destination MAC address (0100.0CCC.CCCC). Já vem habilitado por padrão nos dispositivos Cisco.

Os dispositivos que oferecem suporte ao CDP aprendem informações sobre outros, ouvindo os anúncios CDP.

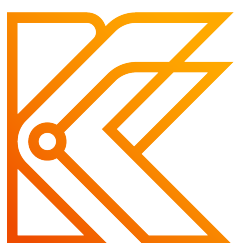
O Link Layer Discovery Protocol (LLDP), definido no padrão IEEE 802.1AB, fornece um protocolo padronizado que fornece os mesmos recursos gerais do CDP. O LLDP tem configuração semelhante e comandos praticamente idênticos em comparação com o CDP. (Não é habilitado por padrão nos dispositivos Cisco). Utiliza o endereço MAC multicast 0180.C200.000E.



```
(1) SW2# show cdp neighbors
(2) Capability Codes: R - Router, T - Trans Bridge, B - Source Route B
(3)                   S - Switch, H - Host, I - IGMP, r - Repeater, P
(4)                   D - Remote, C - CVTA, M - Two-port Mac Relay

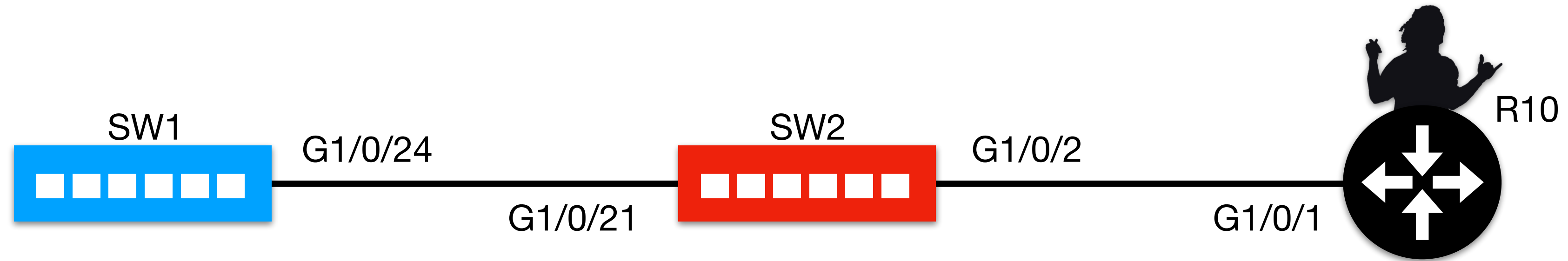
(6) Device ID Local Intrfce Holdtme Capability Platform  Port ID
(7) SW1       Gig 1/0/21   155     S I       WS-C2960X  Gig 1/0/24
(8) R10       Gig 1/0/2   131     R S I     C1111-8P   Gig 0/0/1
(9) Total cdp entries displayed : 2
```

Elementos de camada 1 e dispositivos sem a funcionalidade habilitada se tornam pontos cegos.

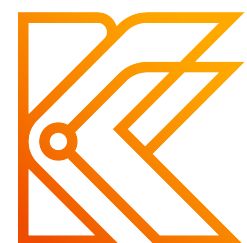
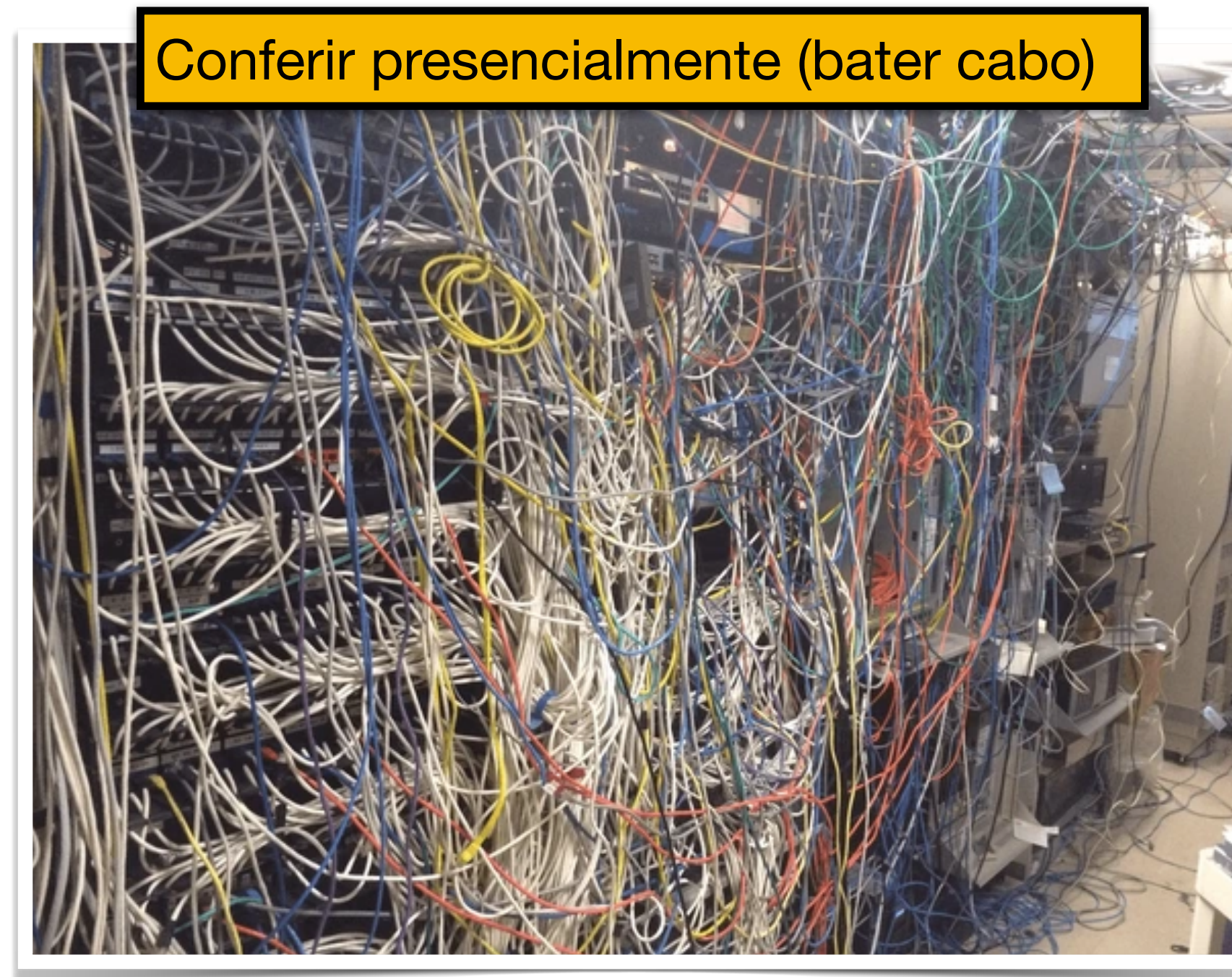




# Tabela MAC, ARP e Bater cabo



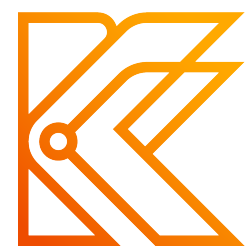
```
(1) SW2# show mac address-table
```





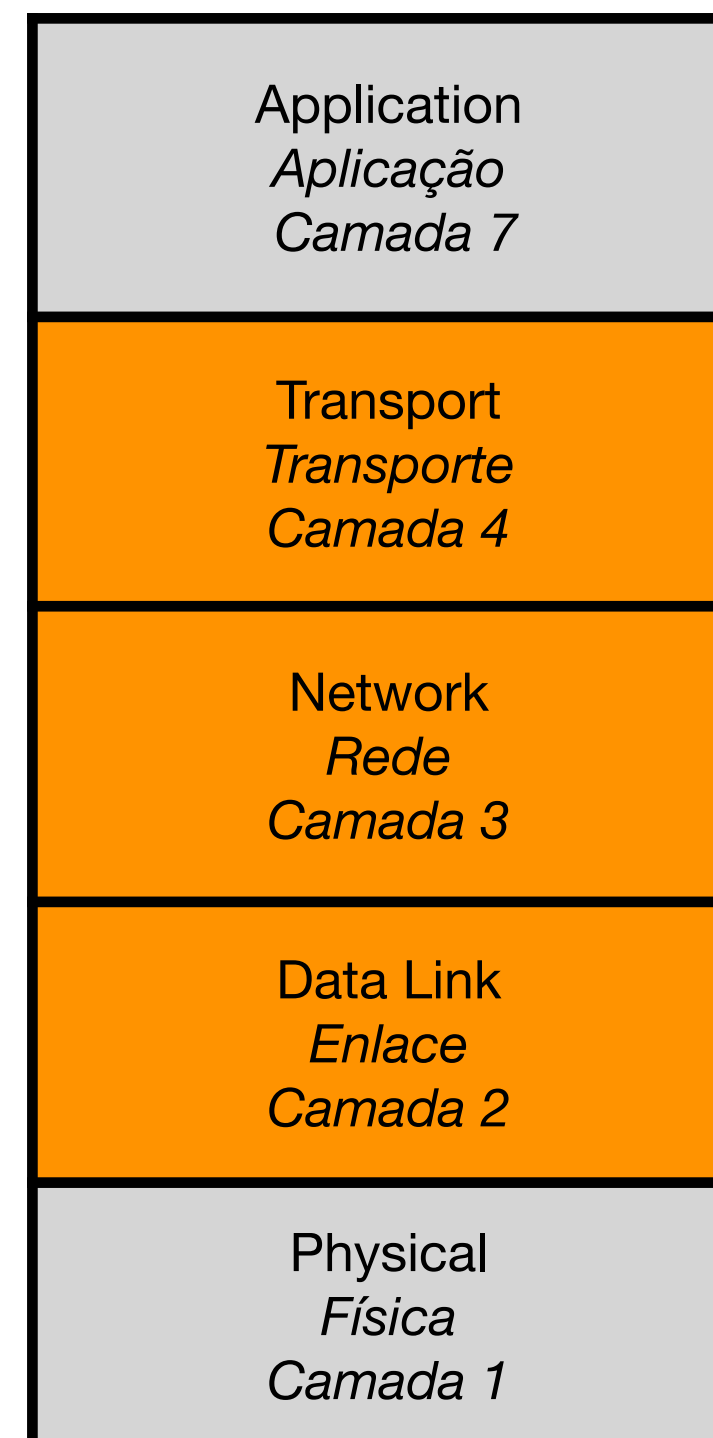
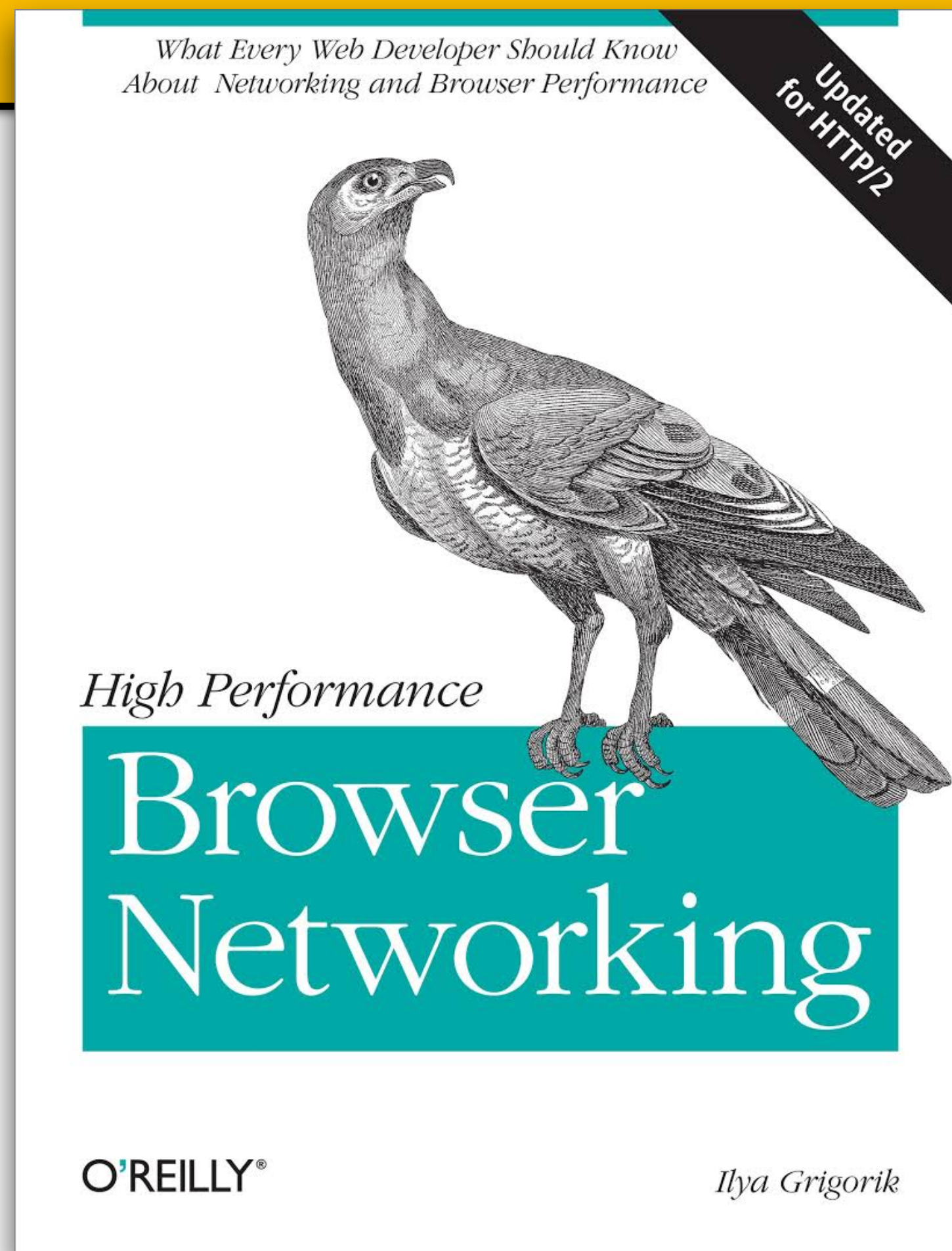
Dica **óbvia** #2:

**Domine os fundamentos.**



"É difícil equilibrar o estudo dos fundamentos da pilha de tecnologia com a necessidade de acompanhar as últimas inovações. E, no entanto, se não entendermos os fundamentos, nosso conhecimento é oco, superficial. Saber como usar as camadas mais altas da pilha de tecnologia não é suficiente. Quando problemas complexos precisam ser resolvidos, quando o inexplicável acontece, a pessoa que entende os fundamentos lidera o caminho".

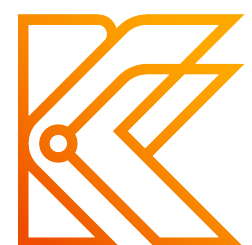
- Steve Souders, Head Performance Engineer, Google 2013



Você consegue responder essas perguntas?

1. Como o switch popula a sua tabela MAC?
2. Como ele escolhe para onde encaminhar o frame?
3. O que é uma porta tagged/untagged?
4. O que é um unknown unicast flooding?
5. Como acontece um loop de camada 2?
6. Por que ethernet é dominante hoje em dia?
7. Como o roteador escolhe a melhor rota?
8. Por que ele analisa o pacote e não o frame?
9. Por que ele reescreve o frame?
10. Por que o modelo fim-a-fim foi quebrado?
11. Por que devemos usar IPv6?
12. Como acontece um loop de camada 3?
13. Para que existe ARP no IPv4 e NDP no IPv6?
14. Qual a diferença de UDP para TCP?
15. Como eu consigo navegar na Internet usando PC?  
Me explique passo a passo.

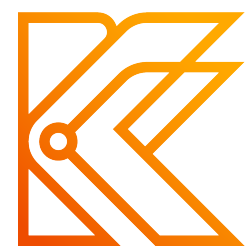
<https://hpbn.co/>



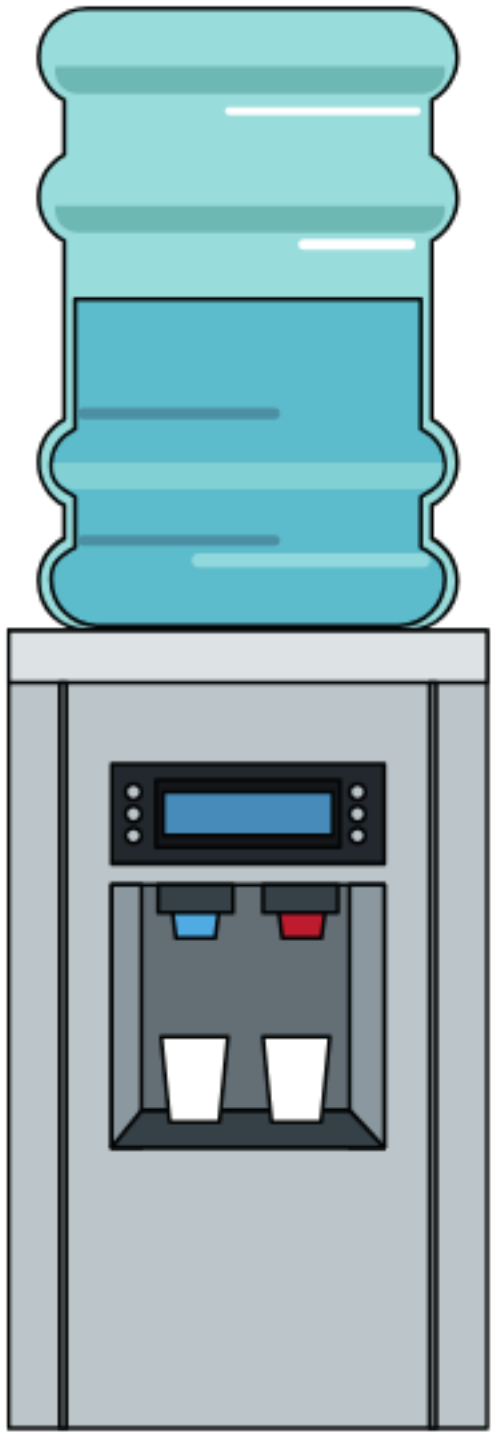


Dica **óbvia** #3:

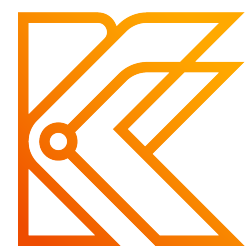
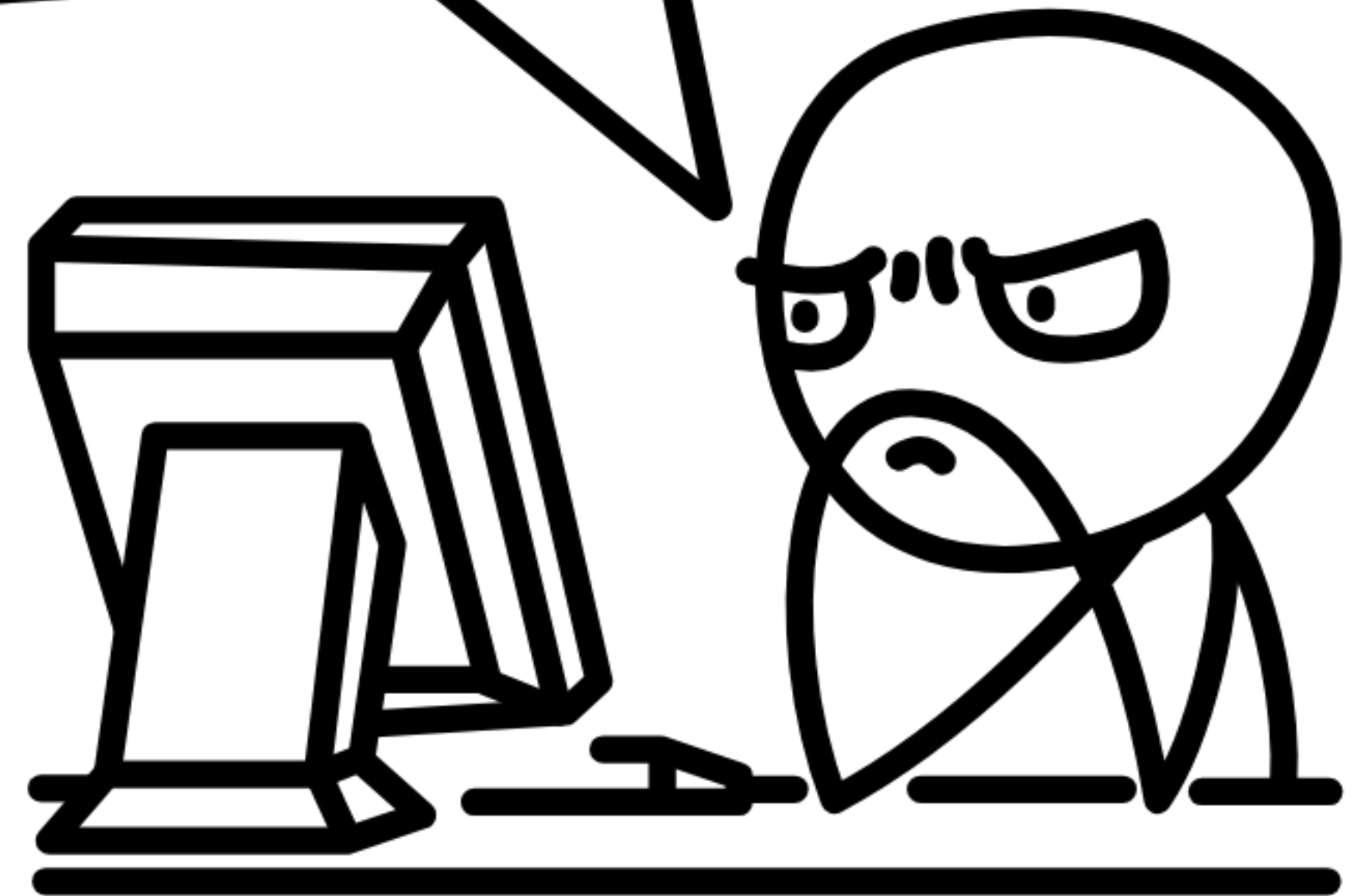
Tenha algum tipo de gestão de mudanças.



# Frases dita por alguém que fez algo errado



A internet caiu  
pra vocês  
também?





# Gestão de Mudanças (Habilitação de Mudança)

ITIL é a sigla para Information Technology Infrastructure Library, que em português significa Biblioteca de Infraestrutura de Tecnologia da Informação. É um conjunto de práticas recomendadas para o gerenciamento de serviços de TI,

A gestão de mudança é uma das 34 práticas de ITIL e tem como objetivo:

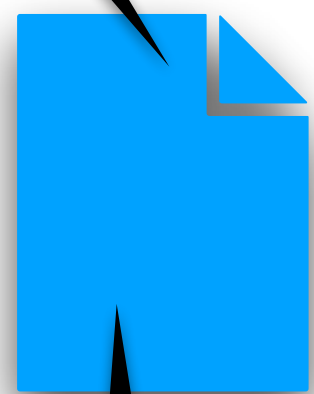
- Controlar o ciclo de vida das mudanças,
- minimizar interrupções nos serviços de TI,
- manter a operação estável,
- empregar métodos e procedimentos padronizados.

Mudanças Padrão: Mudanças pré-autorizadas de baixo risco que seguem um procedimento bem conhecido.

Mudanças de Emergência: Mudanças que devem ser implementadas imediatamente, por exemplo, para resolver um Incidente Grave.

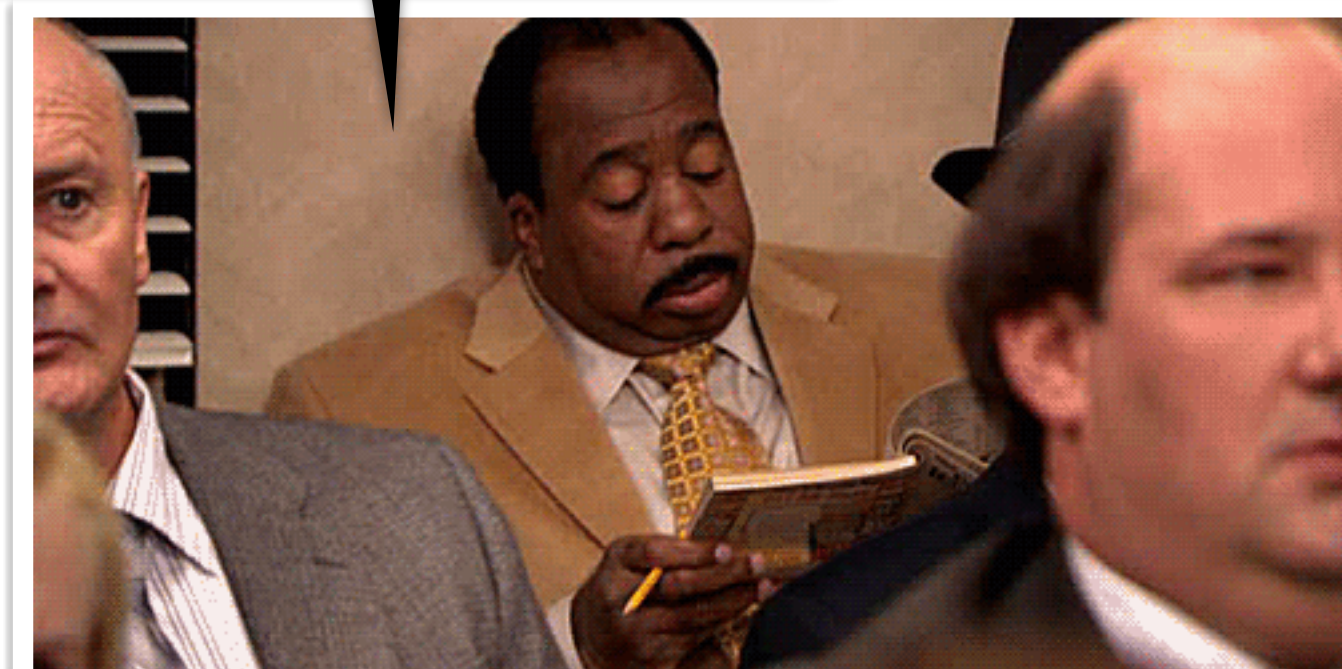
Mudanças Normais: Todas as outras Mudanças que não são Mudanças Padrão ou Mudanças de Emergência.

Requisição de Mudança;



- O que será feito;
- Como será feito;
- Risco de não fazer;
- Risco de fazer;
- Se a mudança não der certo?

Mudança será analisada;



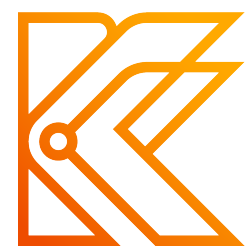
Caso seja aprovado você executa.



Pra que isso?

Dica **óbvia** #4:

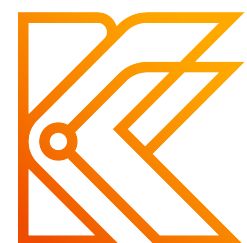
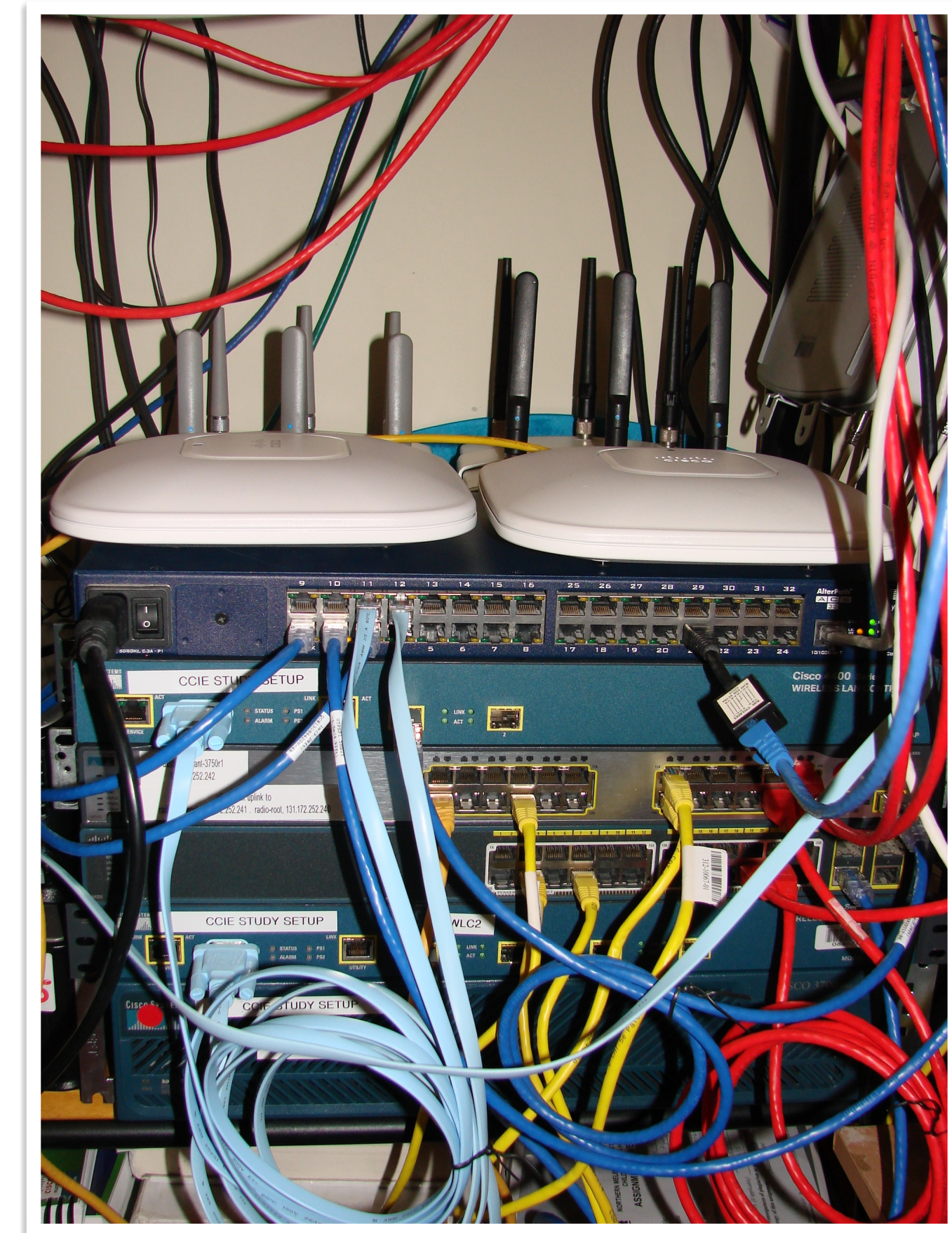
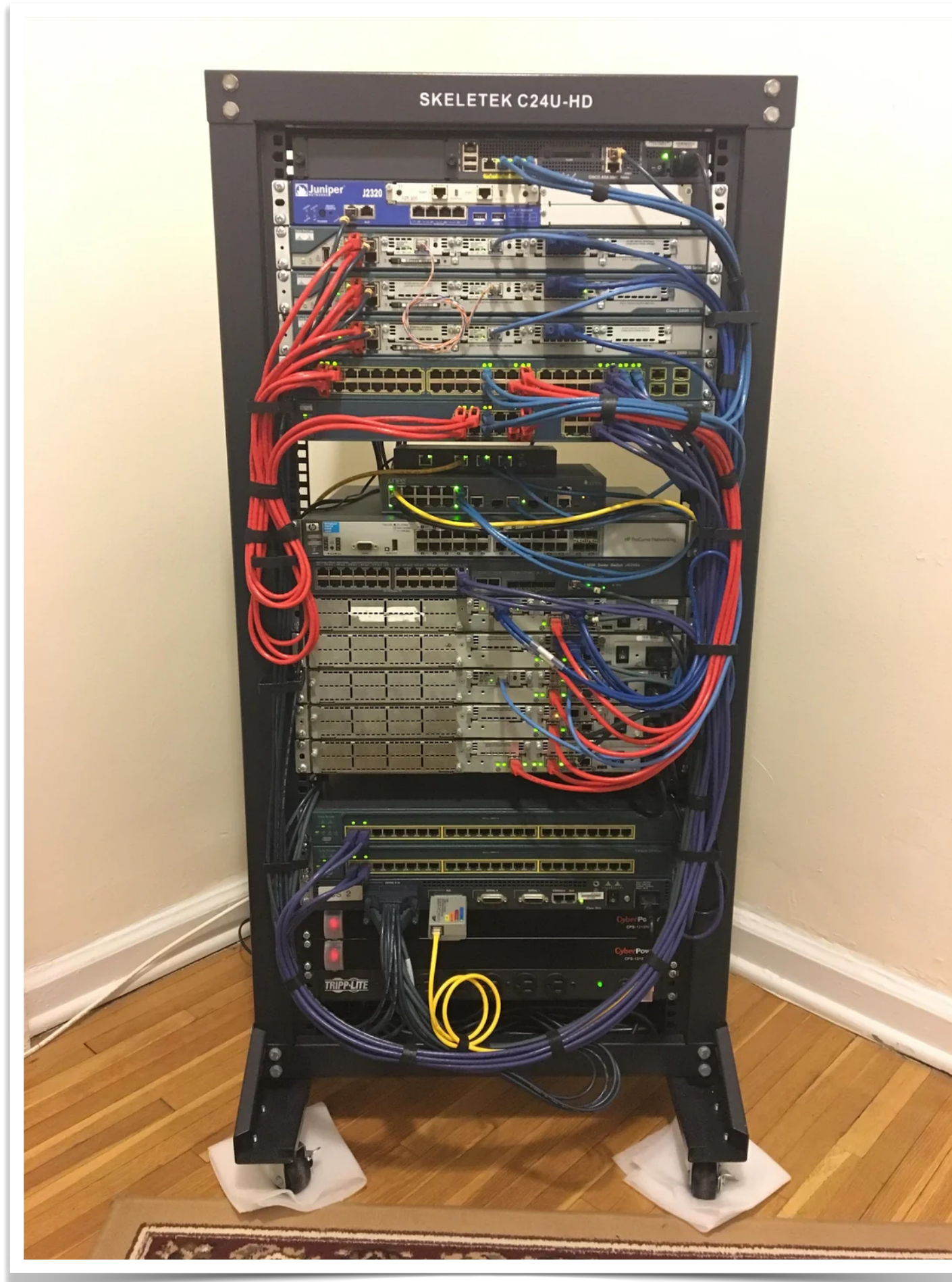
**Tenha ambiente de LAB/Teste/  
Homologação.**





# Home Lab

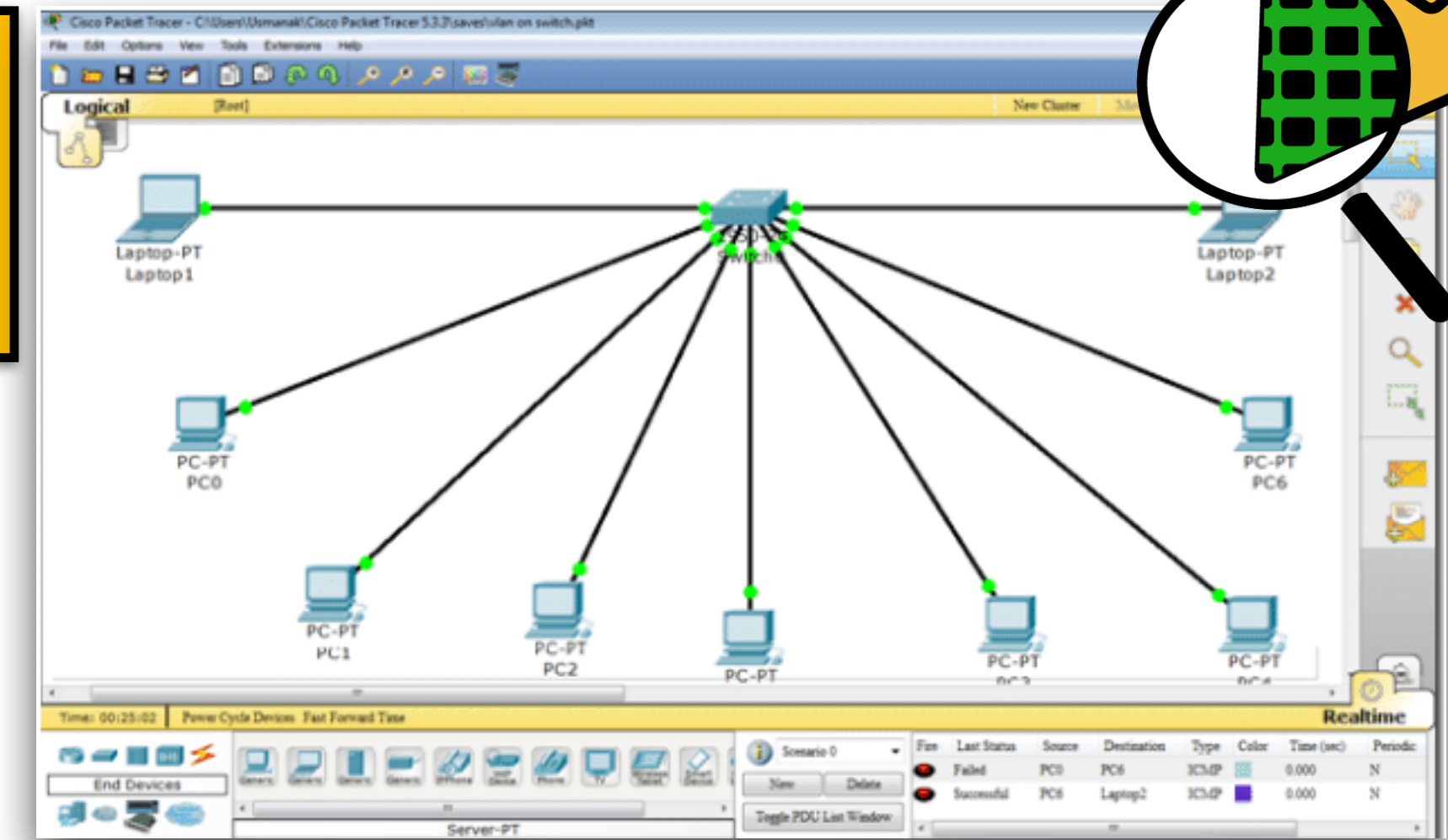
Em redes de computadores o aprendizado era construído através do estudo dos conceitos e da prática em equipamentos caros e de difícil aquisição, isso tornava todo o processo de estudo voltado para o mundo real muito complicado já que o estudante em fase inicial ainda não estava inserido no mercado de trabalho e portanto sem acesso aos dispositivos de rede, a alternativa era comprar equipamentos usados e caros para montar um lab em casa, uma barreira de entrada muito alta.





# Simulador e Emulador

Para diminuir essa barreira em 2005 a Cisco lançou um software chamado Packet Tracer que oferecia dispositivos de rede simulando dispositivos reais através de software, ele não oferecia emulação completa de um hardware de rede mas já era uma revolução para os estudantes.



Por volta de 2007 temos o primeiro emulador para dispositivos de rede Cisco o Dynagen/Dynamips. Agora era possível emular o hardware de roteadores Cisco 1700, 2600, 2691, 3600, 3725, 3745, e 7200 com o sistema operacional real e completo da Cisco limitado apenas pela capacidade do computador onde o emulador era instalado, toda a configuração era feita através de arquivos texto e sem nenhuma interface gráfica, emular switches também não era possível.

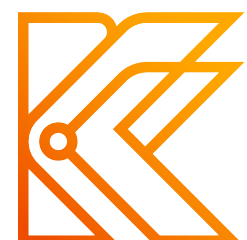
```
(1) [[ROUTER R1]]  
(2) console = 2001  
(3) f0/0 = LAN 1  
(4) f1/0 = LAN 2
```

```
(1) [[ROUTER R2]]  
(2) console = 2001  
(3) f0/0 = LAN 1  
(4) f1/0 = LAN 2
```

```
c:\ Dynagen  
Reading configuration file...  
Warning: Starting R1 with no idle-pc value  
Warning: Starting R2 with no idle-pc value  
Network successfully started  
Dynagen management console for Dynamips  
=> list  
Name      Type      State      Server      Console  
R1        7200      running    localhost:7200 2000  
R2        7200      running    localhost:7200 2001  
=> console R1  
=> help  
  
Documented commands (type help <topic>):  
=====
```

capture	exit	help	import	push	resume	shell	stop	ver
clear	export	hist	list	py	save	show	suspend	
console	filter	idlepc	no	reload	send	start	telnet	

```
=> _
```





# Emuladores

As coisas só melhoraram, logo depois o GNS3 foi apresentado para a comunidade e agora havia uma interface gráfica para o Dynamips;



Depois o UNETLAB apareceu e toda complexidade de configuração do GNS3 desapareceu, agora bastava ligar uma máquina virtual e tudo estava lá disponível através de um simples navegador, nessa época também apareceram as imagens leves de dispositivos Cisco baseadas em Unix/Linux e com suporte a switch (IOL images), agora era possível emular switches L2 e seus protocolos.

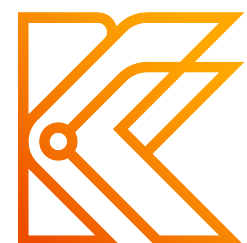
Recentemente ainda tivemos o EVE-NG com recursos mais avançados que o UNETLAB como suporte a imagens QEMU e centenas de dispositivos de rede como firewalls e balanceadores.



Por último o PNETLAB que conta com todos os recursos do EVE PRO e ainda tem uma biblioteca de labs preparados para estudo.

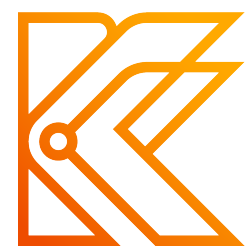
Em pouco menos de 15 anos saímos de zero possibilidade de emular dispositivos de rede para uma variedade de emuladores e facilidades que nenhum profissional sonhava ser possível.

Não tem mais desculpa pra ficar testando as coisas em produção.



Dica **óbvia** #5:

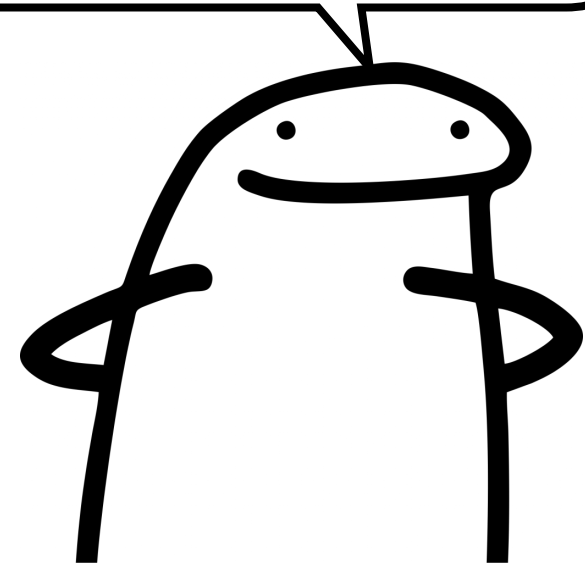
**Elimine ao máximo as gambiarras.**



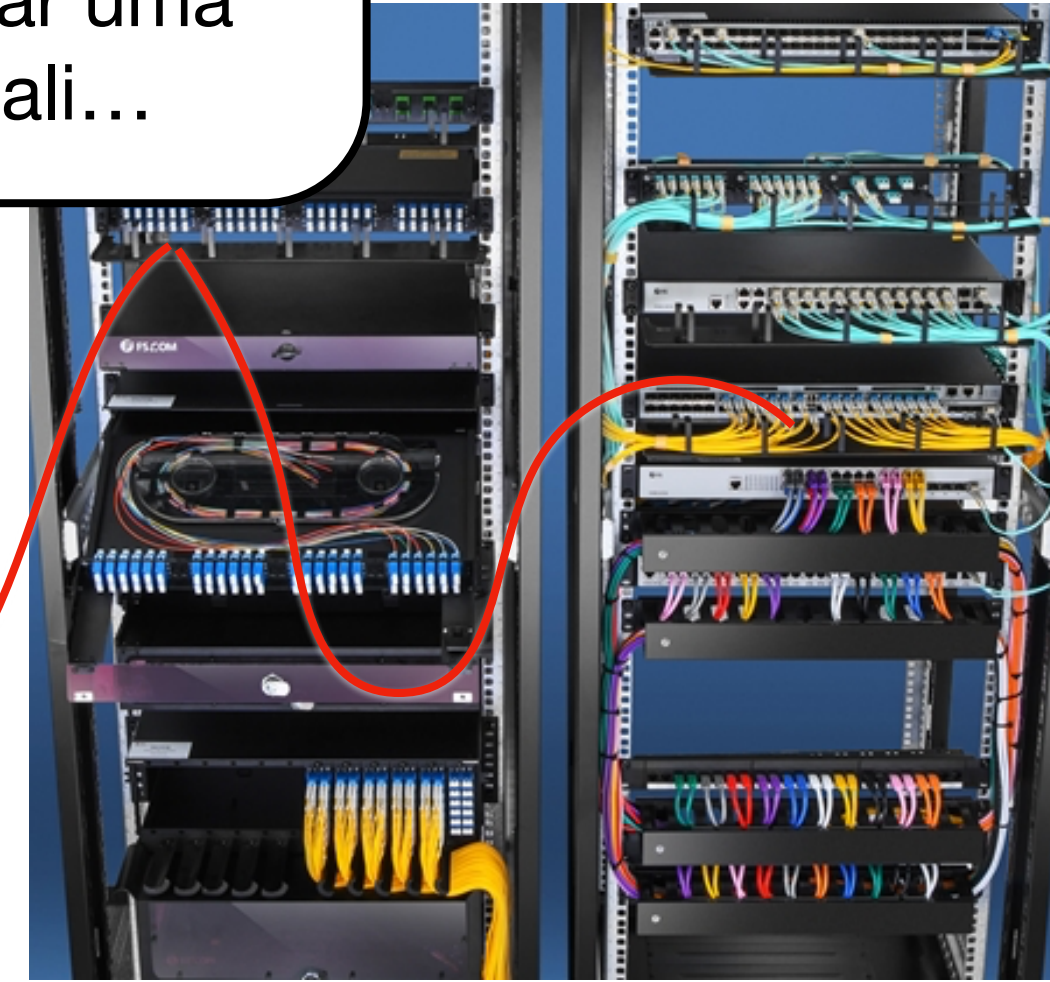
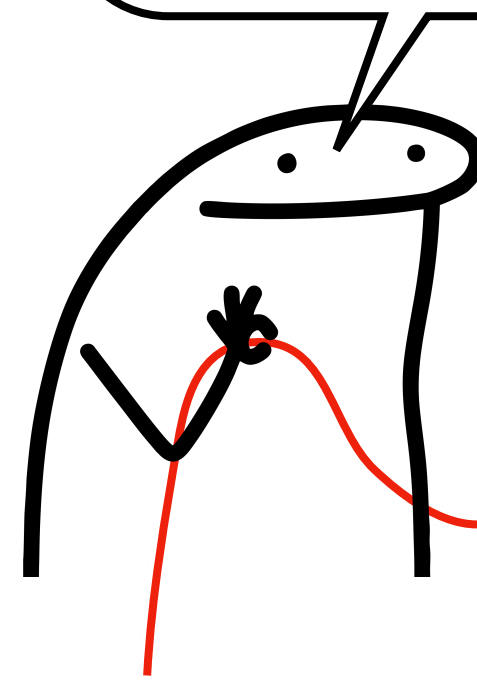


# 2024

Não é melhor passar esse cabo certinho nas guias?

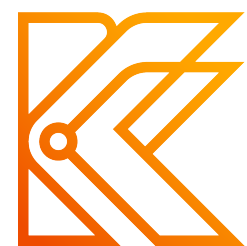
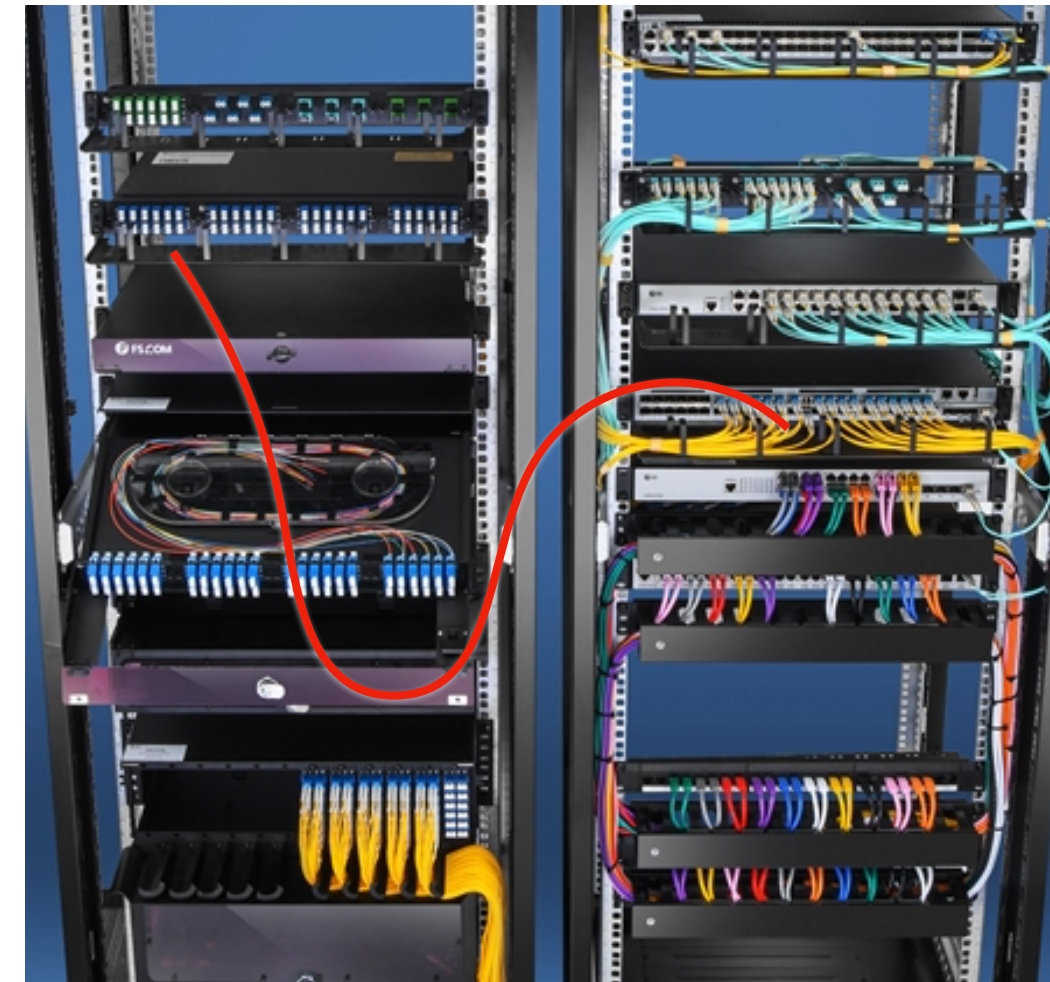
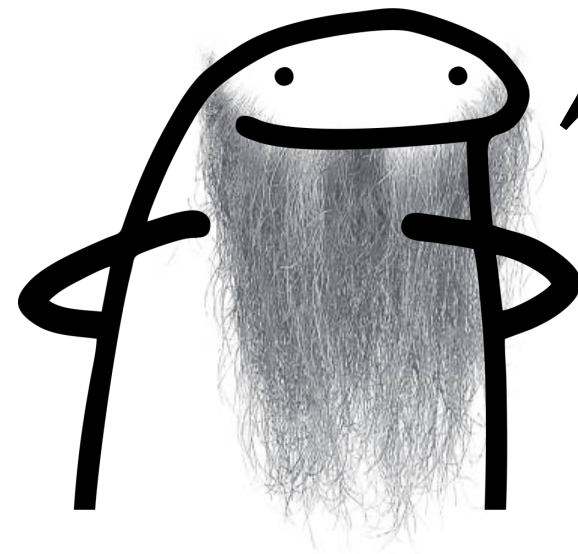


Isso aqui é temporário, só vou testar uma coisinha ali...



# 2054

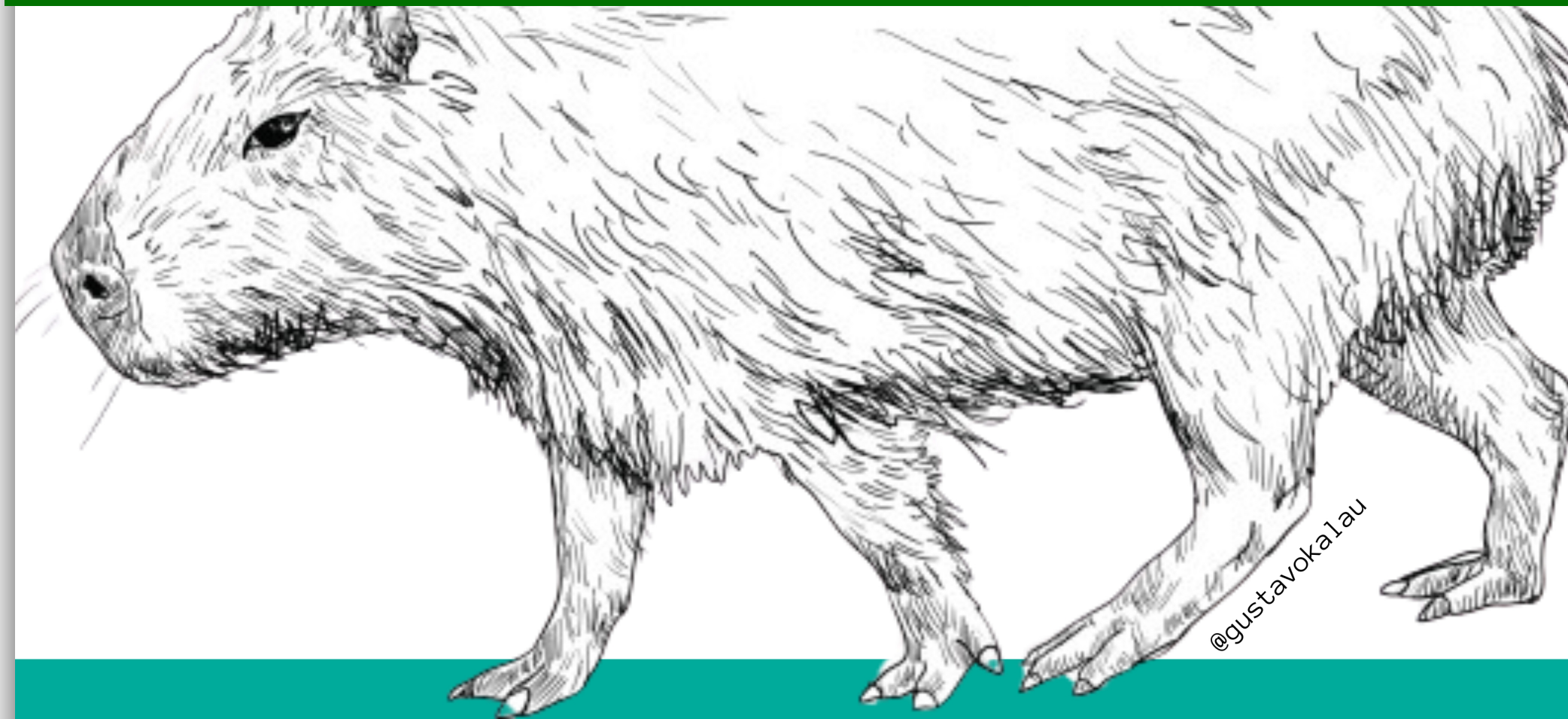
O que será que esse cabo tá ligando? Não tem nada na documentação...



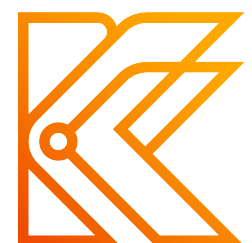


“Uma abordagem realista”

FAKE - É UMA PIADA



Redes de  
Computadores  
Na base da gambiarra

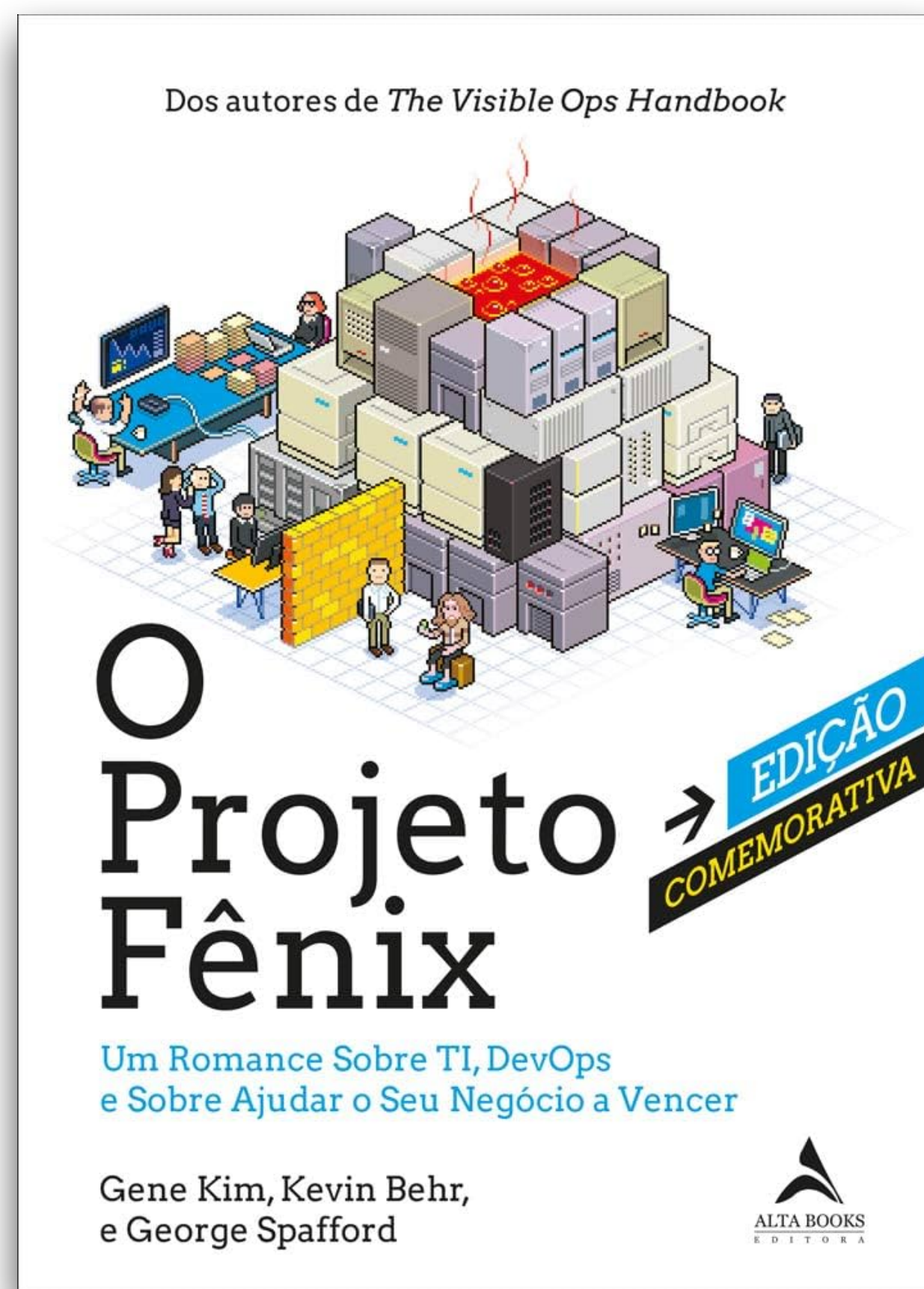




# Gambiarra nos leva a Dívida Técnica

Termo muito utilizado em desenvolvimento de software mas que pode muito bem ser utilizado no nosso mundo.

Dívida técnica refere-se aos custos futuros de retrabalho ou manutenção que surgem da priorização da velocidade e dos atalhos em detrimento da qualidade da rede dimensionamento e infraestrutura adequada, com a dívida acumulando ao longo do tempo e exigindo recursos muito maiores para ser paga.



```
(1) Jun  9 17:54:59.962: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 15 on GigabitEthernet1/2 VLAN200.
(2) Jun  9 17:54:59.962: %SPANTREE-2-BLOCK_PVID_PEER: Blocking GigabitEthernet1/2 on VLAN0015. Inconsistent peer vlan.
(3) Jun  9 17:54:59.962: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet1/2 on VLAN0200. Inconsistent local vlan.
(4) Jun  9 17:55:00.818: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

- Tava com esse log de STP, ai desabilitei o STP e resolveu.

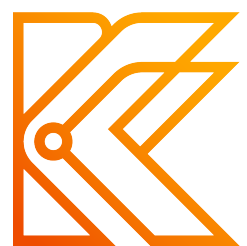
Como tentar diminuir as gambiarras?

- Processos bem definidos;
- Guias/modelos de configuração;
- Treinamento;
- Conscientização;
- Limpeza de configuração desnecessária;
- Revisão de configuração;
- Melhores práticas.



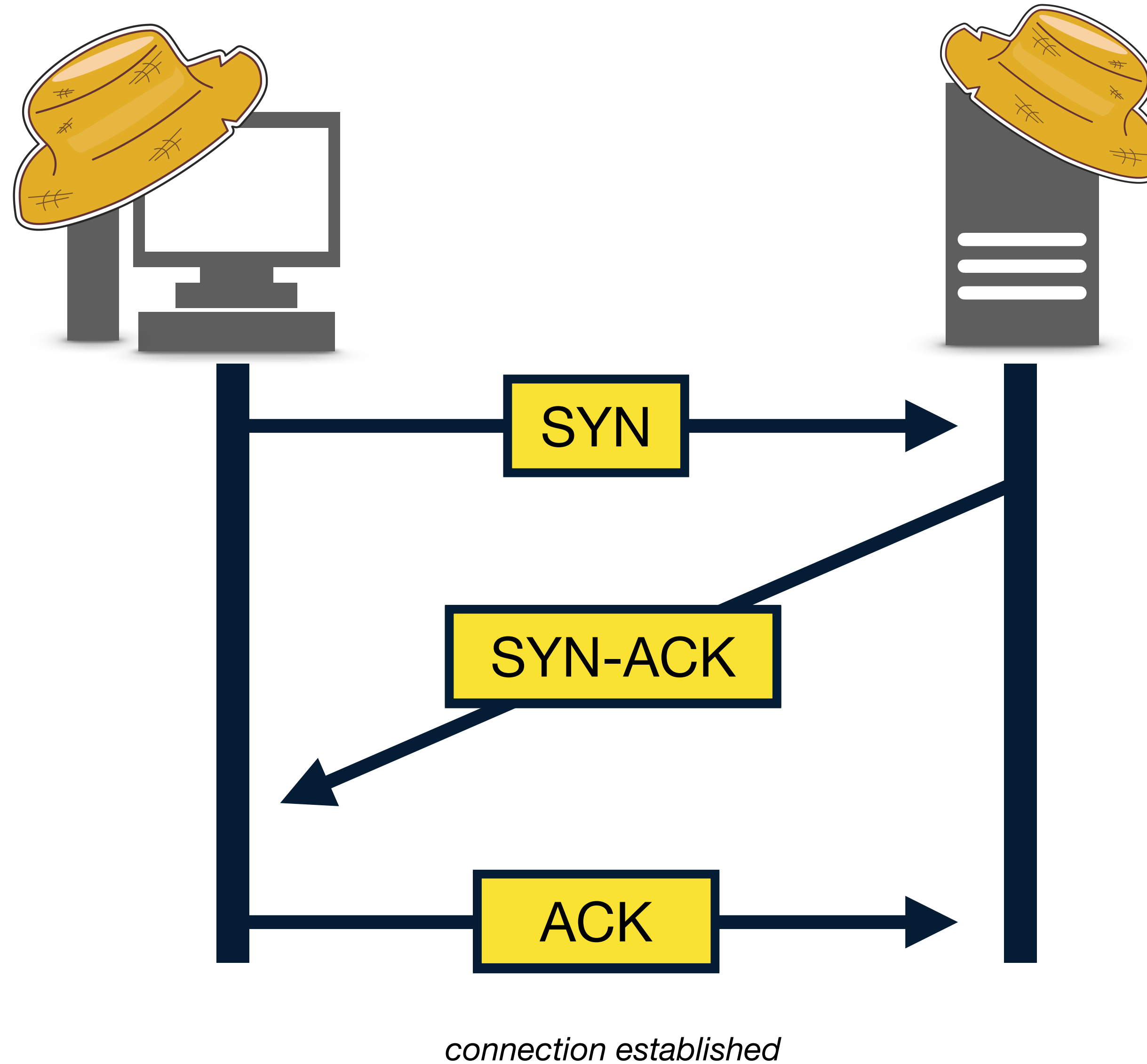
Dica **óbvia** #6:

**Sua rede pode atacar outras redes (não deixe isso acontecer).**

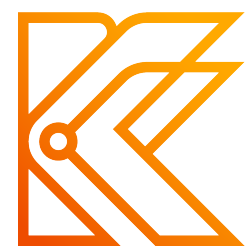
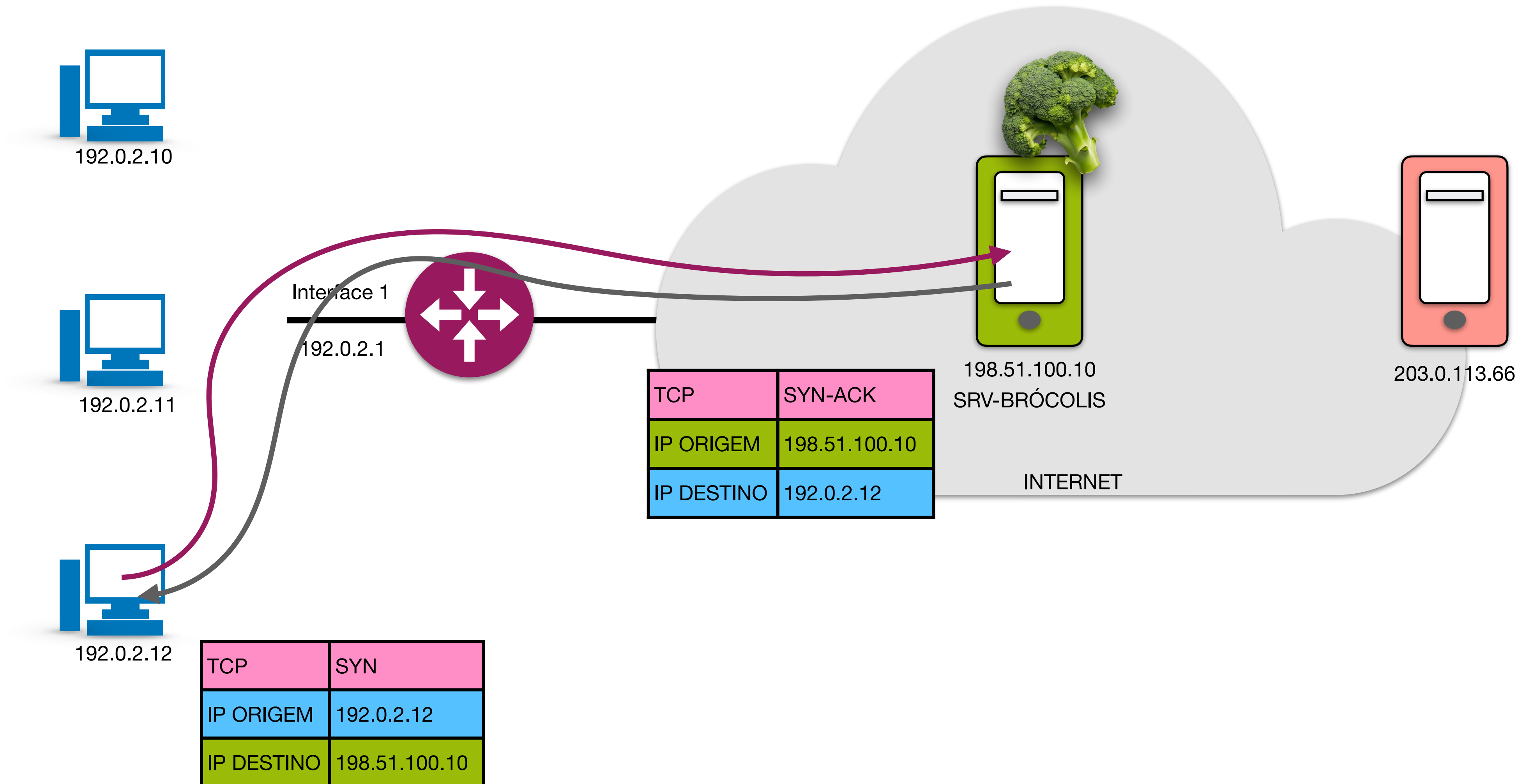




# TCP 3-WAY HANDSHAKE

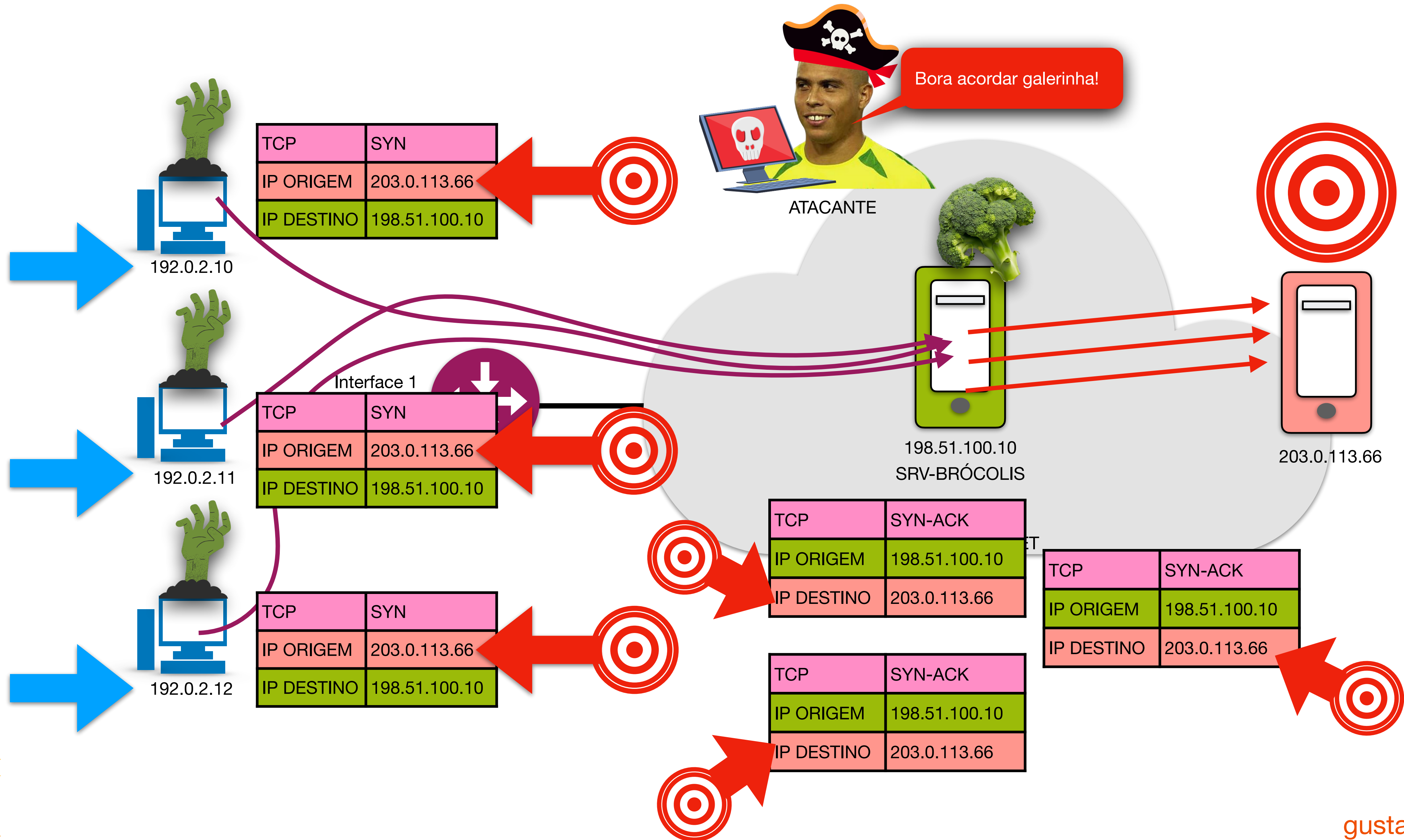


# Comunicação Normal





# Exemplo de IP spoofing e reflexão



# uRPF Unicast Reverse Path Forwarding

Proteção contra ataques de IP spoofing, que normalmente são utilizados em ataques de negação de serviço.

Strict Mode (v1): Dois critérios devem ser atendidos para o tráfego ser encaminhado.

1 - Deve existir alguma entrada válida na tabela de roteamento para esta origem.

2 - A interface para alcançar origem deste pacote deve ser a mesma em que o pacote chegou.

```
router(conf)#interface 1  
router(conf-if)#ip verify unicast source reachable-via rx
```

1 - Existe uma entrada na tabela de roteamento para esse IP de origem?

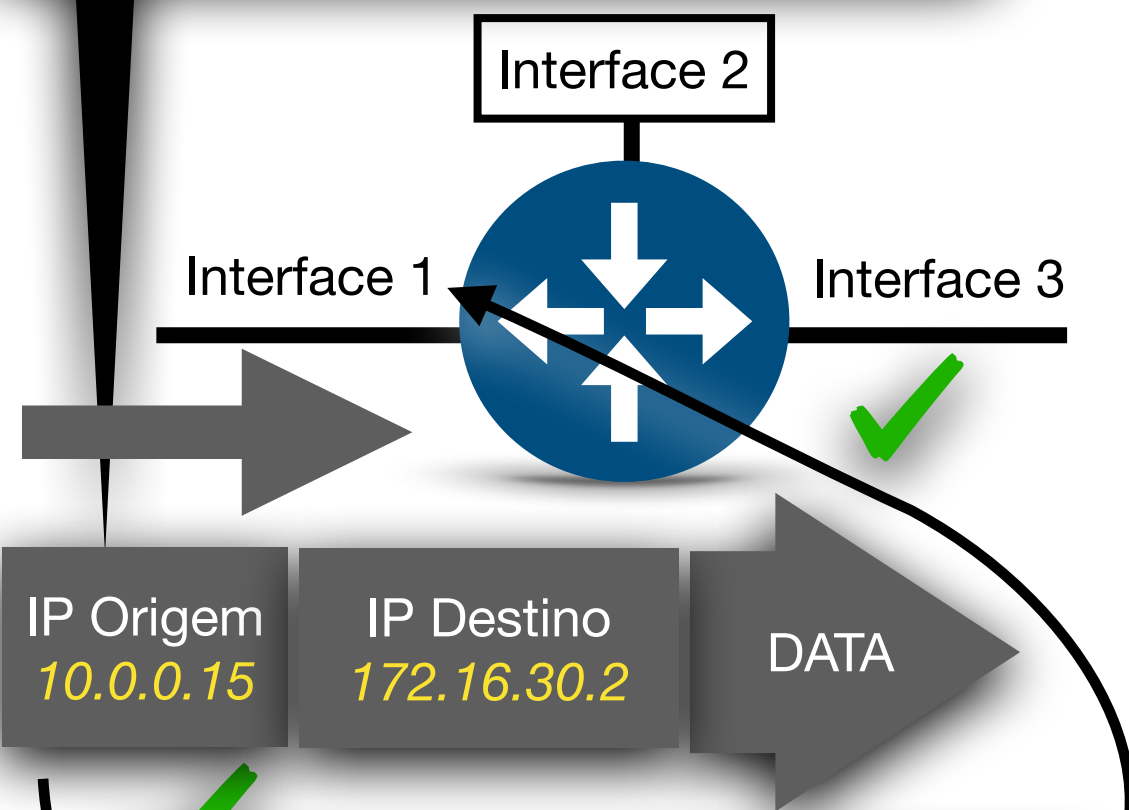


Tabela de Roteamento  
10.0.0.0/24 via Interface 1  
192.168.10.0/24 via Interface 2  
172.16.30.0/24 via Interface 3

2 - A interface para alcançar o IP de origem deste pacote é a mesma em que esse pacote chegou?

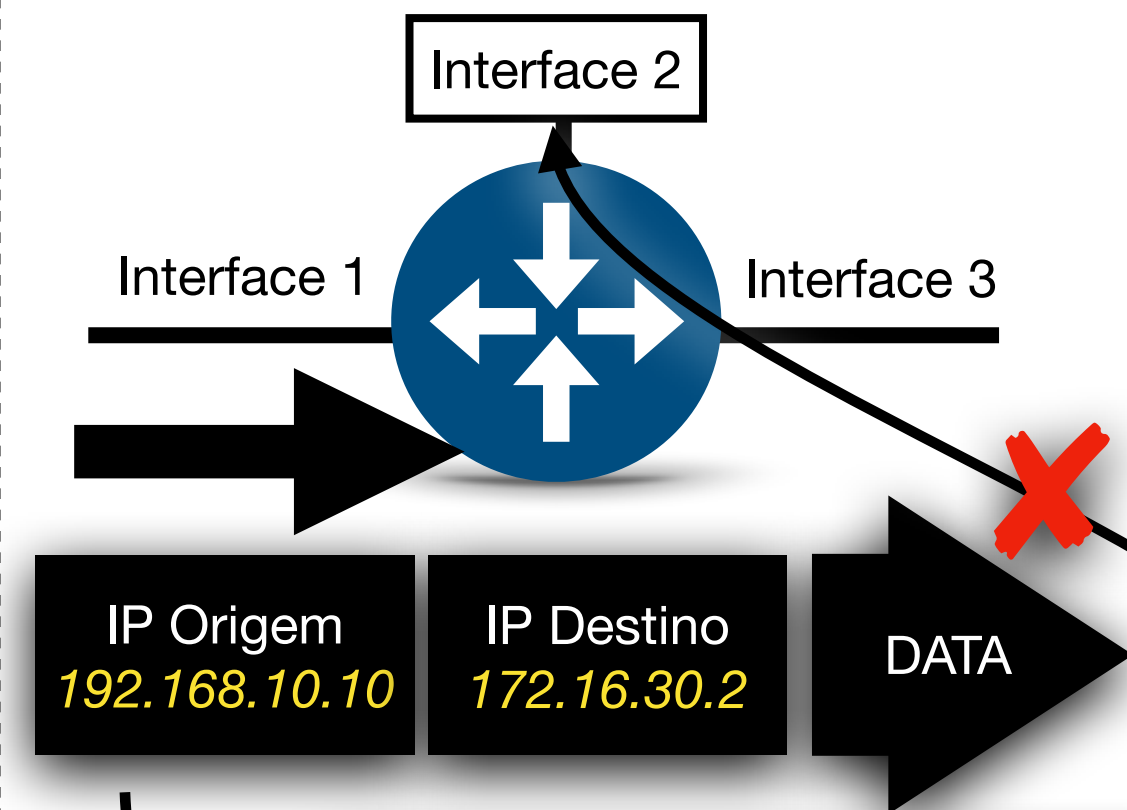


Tabela de Roteamento  
10.0.0.0/24 via Interface 1  
192.168.10.0/24 via Interface 2  
172.16.30.0/24 via Interface 3

Loose Mode (v2): Apenas um critério deve ser atendido.

1 - Deve existir alguma entrada válida na tabela de roteamento para esta origem.

```
router(conf)#interface 1  
router(conf-if)#ip verify unicast source reachable-via any
```

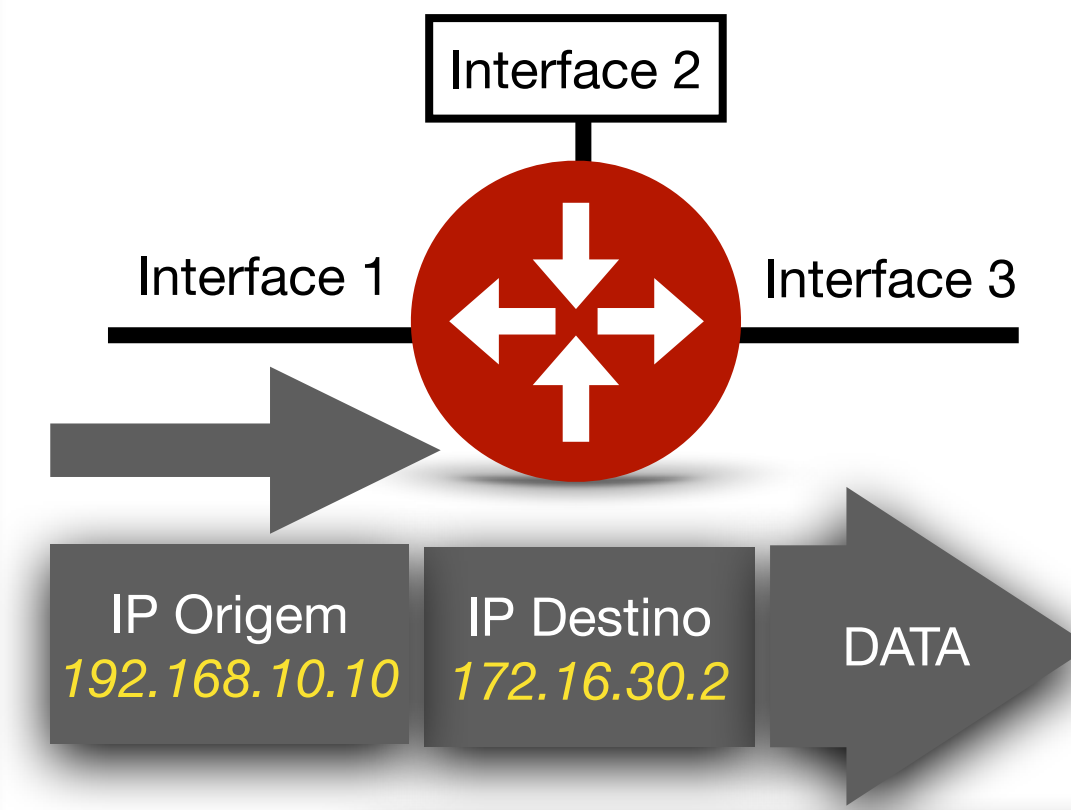


Tabela de Roteamento  
10.0.0.0/24 via Interface 1  
192.168.10.0/24 via Interface 2  
172.16.30.0/24 via Interface 3

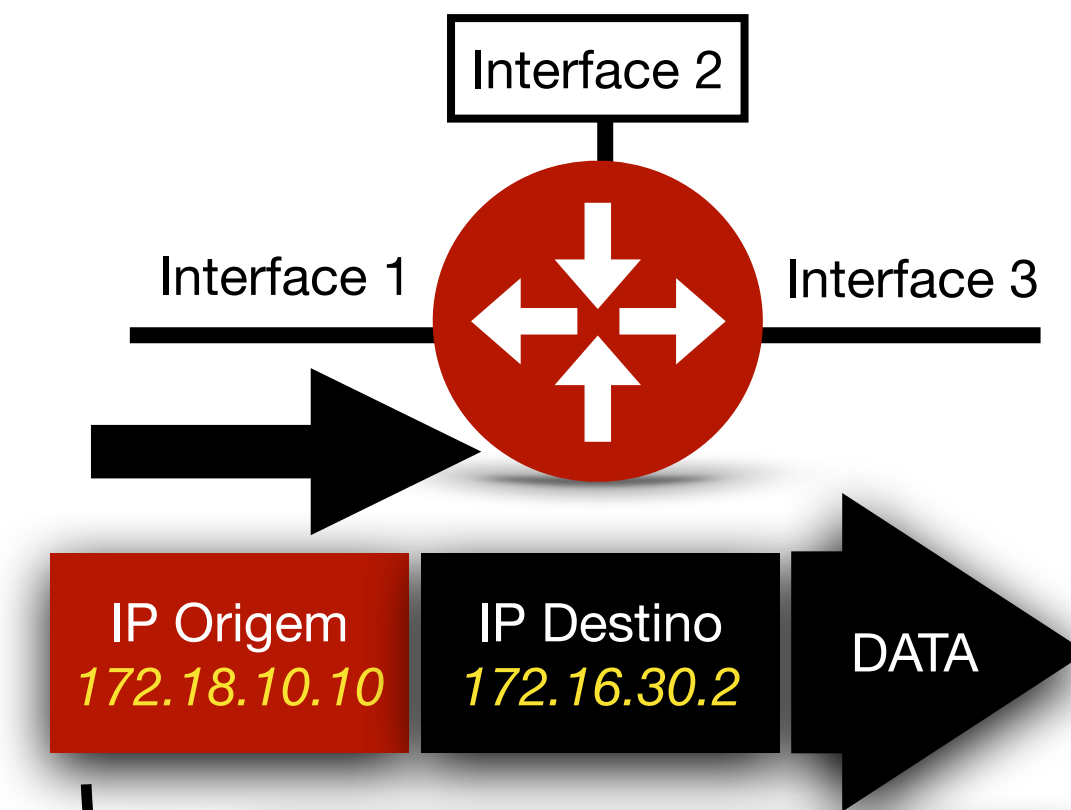


Tabela de Roteamento  
10.0.0.0/24 via Interface 1  
192.168.10.0/24 via Interface 2  
172.16.30.0/24 via Interface 3


Existe a opção allow-default, usada quando o caminho de retorno está associado a uma interface escolhida com base em uma rota default. Por padrão, ele é descartado.



# Obrigado! Perguntas?

 [youtube.com/gustavokalau](https://youtube.com/gustavokalau)

 [linkedin.com/in/gustavokalau/](https://linkedin.com/in/gustavokalau/)

 [t.me/GustavoKalauRiscoZero](https://t.me/GustavoKalauRiscoZero)

 [instagram.com/gustavokalau/](https://instagram.com/gustavokalau/)

NEWSLETTER: [gustavokalau.beehiiv.com/](https://gustavokalau.beehiiv.com/)

